Juridische kwalificatie van verkeersgegevens in het licht van artikel 13 Grondwet

Koops, E.J.

Publication date:
2013

Document Version
Publisher's PDF, also known as Version of record

UNIVERSITEIT VAN TILBURG

Juridische kwalificatie van verkeersgegevens in het licht van artikel 13 Grondwet

Bert-Jaap Koops

Universiteit van Tilburg
TILT – Tilburg Institute for Law, Technology, and Society
Postbus 90153
5000 LE Tilburg
<e.j.koops@uvt.nl>

februari 2013

Colofon

Auteur
prof.dr. Bert-Jaap Koops

Uitgave
Universiteit van Tilburg
TILT – Tilburg Institute for Law, Technology, and Society
Postbus 90153
5000 LE Tilburg

Opdrachtgever
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Datum
februari 2013

Inhoudsopgave

Lijst met tabellen

Afkortingen

BSN	BurgerServiceNummer
BVerfG	Bundesverfassungsgericht [Duits federaal constitutioneel hof]
BZK	Binnenlandse Zaken en Koninkrijksrelaties
EDI	Electronic Data Interchange
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag van de Rechten van de Mens
GPS	Global System for Mobile communications
Gw	Grondwet
HR	Hoge Raad
ICT	informatie- en communicatietechnologie
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISP	Internet Service Provider
NAW	naam, adres, woonplaats
PTT	Posterijen, Telegrafie en Telefonie
Sr	Wetboek van Strafrecht
Stb.	Staatsblad
Sv	Wetboek van Strafvordering
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol [spraaktelefonie via Internet]
Wbp	Wet bescherming persoonsgegevens
Wiv 2002	Wet op de inlichtingen- en veiligheidsdiensten 2002
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum
WPolG	Wet Politiegegevens

1. Inleiding

1.1. Achtergrond

De wetgever beoogt om artikel 13 Grondwet – het huidige brief-, telefoon- en telegraafgeheim – te actualiseren.[1] In oktober 2012 is een concept-wetsvoorstel in consultatie gegeven.[2] In dat wetsvoorstel worden verkeersgegevens – gegevens als wie met wie wanneer belt of mailt – uitgesloten van bescherming onder artikel 13, omdat zij niet de inhoud van communicatie betreffen. Wanneer verkeersgegevens echter wel geheel of ten dele mede op de inhoud van de communicatie betrekking hebben, zouden zij als inhoud moeten worden behandeld. In de praktijk is het niet eenvoudig om te bepalen wanneer verkeersgegevens (mede) op inhoud betrekking hebben.

Daarom heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een onderzoek uitgezet naar de huidige betekenis en eventuele problemen bij de technische en juridische kwalificatie van verkeersgegevens in het licht van de bescherming van artikel 13 Grondwet. Het onderzoek zou een juridische en een technologische component moeten bevatten. De juridische component concentreert zich op het in kaart brengen van de juridische kwalificatie van verkeersgegevens, terwijl bij de technologische component van het onderzoek de technische kwalificatie van verkeersgegevens in kaart wordt gebracht. Dit rapport biedt de verslaglegging van de juridische component van het onderzoek; de technologische component is parallel hieraan uitgevoerd door Jan Smits.[3] Beide onderzoeken samen beogen een beeld op te leveren in hoeverre het vanuit technologisch en juridisch opzicht mogelijk is verkeersgegevens in het grijze gebied tussen verkeersgegevens en inhoud te kwalificeren in het licht van de herziening van artikel 13 Gw.

1.2. Doelstelling en vraagstelling

De **doelstelling** van dit onderzoek is eventuele probleemgevallen bij de juridische kwalificatie te identificeren, eventuele discrepanties tussen de technische en juridische duiding van verkeersgegevens te inventariseren, en – voor zover haalbaar en relevant – oplossingsrichtingen te schetsen voor de bescherming van verkeersgegevens in wetgeving.
De **vraagstelling** luidt: welke typen verkeersgegevens moeten juridisch beschermwaardig worden geacht onder artikel 13 Gw, gelet op de ratio en functie van artikel 13, en in hoeverre zijn deze typen juridisch af te bakenen op een manier die verenigbaar is met de technische realiteit?

Het onderzoek wordt geordend aan de hand van de volgende deelvragen die tezamen een antwoord geven op de algemene vraagstelling.

1. Wat is de 'inhoud' van communicatie, gelet op de ratio en functie van bescherming door artikel 13 Gw? Gaat het bijvoorbeeld om de hele inhoud of ook delen ervan, om letterlijke inhoud of om strekking?
2. Welke grijze gebieden bestaan er tussen verkeersgegevens en inhoud van communicatie?
3. Kunnen verkeersgegevens in de grijze gebieden worden geclassificeerd in een typologie van verschillende manieren waarop verkeersgegevens samenhangen met inhoud?
4. Welke typen verkeersgegevens, volgens de typologie uit vraag 3, zijn beschermwaardig onder artikel 13 Gw omdat zij 'inhoud' betreffen volgens het antwoord op vraag 1?
5. Welke aandachtspunten kunnen worden geformuleerd voor de keuzes die de wetgever moet maken ten aanzien van verkeersgegevens in het licht van de herziening van artikel 13 Gw?

[1] Zie *Kamerstukken II* 2011/12, 31 570, nrs. 20-21. Over de (lange) voorgeschiedenis, zie Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, 2010 en de bespreking daarvan in *Tijdschrift voor Constitutioneel Recht* 2011 nr. 2, met verwijzingen.
[2] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, http://www.internetconsultatie.nl/briefentelecommunicatiegeheim (geraadpleegd 15 januari 2013).
[3] Smits 2013.

1.3. Afbakening

Het onderzoek vindt plaats in het kader van het concept-wetsvoorstel ter aanpassing van artikel 13 Gw (hierna: wetsontwerp-2012).[4] In dat wetsontwerp worden, in navolging van de commissie-Franken en de commissie-Thomassen, verkeersgegevens als zodanig uitgesloten van de bescherming van artikel 13 Gw, aangezien zij geen inhoud van communicatie betreffen. Alleen voor zover verkeersgegevens raken aan de inhoud van communicatie, zouden ze beschermwaardig kunnen zijn onder artikel 13. Dit onderzoek ziet daarom niet primair op de vraag of verkeersgegevens *als zodanig* bescherming behoeven onder artikel 13 Gw, hoewel die vraag niet helemaal losgekoppeld kan worden van de vraag naar de ratio en reikwijdte van artikel 13 Gw. Daarom wordt wel enige aandacht besteed aan de beschermwaardigheid van verkeersgegevens onder artikel 13 Gw in het algemeen, maar de nadruk ligt op de vraag onder welke omstandigheden verkeersgegevens zodanig verbonden zijn met inhoud van communicatie dat zij aanspraak kunnen maken op het beschermingsregime van communicatie-inhoud onder artikel 13 Gw.

1.4. Terminologie

Ter aanduiding van datgene wat artikel 13 Gw beoogt te beschermen, wordt in dit rapport kortheidshalve de term 'correspondentiegeheim' gebruikt. Dit sluit aan bij artikel 8 EVRM, dat de term 'correspondence' hanteert. Hiermee beoog ik niet om een nieuw begrip te introduceren in de discussie over artikel 13 Gw, maar simpelweg om een compact begrip voorhanden te hebben dat als koepelterm kan fungeren voor de verschillende termen die in de literatuur en wetgeving worden gebruikt (zoals brief-, telefoon- en telegraafgeheim; brief- en telecommunicatiegeheim; communicatiegeheim). Waar in dit rapport 'correspondentiegeheim' wordt gebruikt, moet dus gelezen worden de term die in de context door de desbetreffende auteur wordt gehanteerd om het beschermingsobject van artikel 13 Gw aan te duiden.

Onder 'verkeersgegevens' kunnen als werkdefinitie worden verstaan gegevens die worden verwerkt voor de afhandeling (transport of facturering) van telecommunicatie. (In par. 2.3 worden nadere definities genoemd voor dit begrip.)

1.5. Methoden van onderzoek

Het onderzoek is uitgevoerd op basis van literatuuronderzoek. Het literatuuronderzoek bestond uit een analyse van de wetsgeschiedenis van artikel 13 Gw, van de diverse voorstellen sinds de jaren '90 tot herziening hiervan, alsmede van rapporten en academische literatuur over verkeersgegevens en het correspondentiegeheim.

Het onderzoek is uitgevoerd van november 2012 tot medio januari 2013. De rapportage is afgerond in februari 2013.

[4] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, http://www.internetconsultatie.nl/briefentelecommunicatiegeheim (geraadpleegd 15 januari 2013).

2. De ratio en reikwijdte van artikel 13 Grondwet

Van Dorst heeft opgemerkt dat het opvalt dat bij de behandeling van alle voorstellen die hebben geleid tot het huidige artikel 13 Gw 'nergens een beschouwing is ten beste gegeven over de grondslag van het postgeheim'.[5] De ratio en reikwijdte van artikel 13 Gw kunnen daarom alleen indirect worden afgeleid uit de wetsgeschiedenis en de doctrine. In dit hoofdstuk wordt eerst de wetgeschiedenis besproken, voor zover die aanknopingspunten bevat voor de ratio en reikwijdte, en vervolgens de doctrine. Relevante passages worden geciteerd, waarbij kernformuleringen betreffende de ratio en reikwijdte vet worden weergegeven. Op basis daarvan worden aansluitend de bevindingen samengevat om zicht te krijgen op wat precies aan inhoud van communicatie artikel 13 Gw beoogt te beschermen.

2.1. Wetsgeschiedenis

Bij de invoering van het briefgeheim in 1848 heeft de wetgever geen inhoudelijke argumentatie gegeven: de bepaling 'zal wel geene verdediging behoeven. Dat het geheim der brieven onschendbaar behoort te zijn, is eene bepaling die in de meeste grondwetten van Europa thans is opgenomen. Het gemis daarvan scheen de Nederlandsche Grondwet te ontsieren.'[6] In de wetsgeschiedenis is weinig te vinden over de vraag welk deel van de brief wordt beschermd: de inhoud of ook uiterlijke kenmerken.[7] De argumentatie van Thorbecke, de geestesvader van het briefgeheim uit 1848, suggereert dat het (vooral of alleen?) om de inhoud gaat:

> 'Het **openen of doen openen van iemands brieven** tegen zijnen wil, is geen mindere, ja gevaarlijker aanranding der bijzondere vrijheid, dan wanneer verklikkers in zijn huis worden gezonden, om zijne vertrouwelijke gesprekken af te luisteren, zoodat het, naar het voorbeeld van andere Staten, evenzeer te pas komt, den wetgever te verpligten, dat hij het geheim der brieven, als dat hij de woning van den ingezeten doe eerbiedigen.'[8]

De Staatscommissie die het Wetboek van Strafvordering van 1926 voorbereidde, hanteerde eveneens de interpretatie dat alleen de inhoud werd beschermd: 'De heer SCHIMMELPENNINCK vraagt, **of het brievengeheim niet geacht moet worden zich tot het feit der verzending zelve uit te strekken**? Mag de post van het feit aan den O.v.J. kennis geven? De commissie meent de eerste vraag **ontkennend**, de tweede bevestigend te moeten beantwoorden.'[9] Met andere woorden, verkeersgegevens vallen niet onder de reikwijdte van het briefgeheim zoals ingevoerd in 1848.

Bij de totstandkoming van het huidige artikel 13 Gw ligt de nadruk op het kennisnemen van de inhoud van communicatie:

> 'Er is, naar het de ondergetekenden voorkomt, een belangrijk verschil tussen het brief- en telefoongeheim enerzijds en het telegraafgeheim anderzijds. Communicatie per brief of telefoon kan plaatsvinden zonder dat **de doorgevende instantie van de inhoud van de brief of het telefoongesprek kennis neemt**. Het vertrouwelijk karakter van deze communicatievormen is daardoor duidelijk **en de inhoud van brief en gesprek kan daarop worden afgestemd**.'[10]

> 'Met de staatscommissie en de opstellers van de Proeve van een nieuwe grondwet zijn wij van mening, dat naast de briefwisseling ook de communicatie door middel van telefoon en telegraaf een belangrijke plaats in het maatschappelijk verkeer heeft verworven en **in verband met het privékarakter ervan** onder de grondrechten moet worden opgenomen.[11]

> (…) Dat betekent niet, dat er niet een **zeker karakterverschil tussen deze drie rechten** zou bestaan. Bij het briefgeheim gaat het om een communicatie die plaatsvindt in gesloten enveloppes, althans in een verpakking welke het oogmerk van de afzender tot uitdrukking brengt, **dat derden –**

[5] Van Dorst 1982, p. 287.
[6] *Handelingen II* 1847-1848, p. 350, geciteerd in Hofman 1995, p. 108.
[7] Hofman 1995, p. 149.
[8] *Bijlage Handelingen II* 1844-1845, p. 461, geciteerd in Hofman 1995, p. 107.
[9] Notulen 13e vergadering Staatscommissie, p. 16, Lindenberg 2002, p. 204.
[10] *Kamerstukken II* 1970-71, 11 051, nr. 3, p. 20.
[11] *Kamerstukken II* 1975-76, 13 872, nr. 3, p. 44.

waaronder de PTT – van de inhoud van de brief geen kennis nemen. Bij het telegraafgeheim is dit aspect minder sterk aanwezig. Zo zal het open aangeboden of per telefoon opgegeven **telegram onvermijdelijk ter kennis moeten komen** van hen, die het telegram aannemen, doorzenden of telefonisch afleveren. Het telegraafgeheim komt in die gevallen vooral hierin tot uitdrukking, dat zij, **die ambtshalve van de inhoud van het telegram kennis nemen**, **daarover aan derden geen mededeling mogen doen**.

Het telefoongeheim ligt wat het geheimhoudingsaspect betreft enigszins tussen de beide eerdergenoemde rechten in. Gezien de mate van automatisering van het telefoonverkeer, waardoor voor het telefoongesprek gewoonlijk geen tussenkomst van derden meer nodig is, benadert het telefoongeheim wat het geheimhoudingsaspect betreft het briefgeheim. Anders dan bij de briefwisseling is voor de telefoonverbinding evenwel de instandhouding van een ingewikkelde apparatuur vereist. Het is onvermijdelijk, dat deze apparatuur in haar verschillende onderdelen voortdurend wordt gecontroleerd en waar nodig wordt hersteld. Om te kunnen vaststellen of een verbinding goed verloopt is het echter noodzakelijk, dat op telefoongesprekken wordt ingeluisterd. Het **zou te ver gaan het telefoongeheim zo ruim op te vatten, dat ook deze technische controle en herstelwerkzaamheden, waarbij wel eens iets van een gesprek moet worden opgevangen, als inbreuken** op dit recht zouden worden aangemerkt. Zo ver strekt het in het onderhavige artikel voorgestelde recht zich niet uit; wel brengt het artikel mee, dat **hetgeen aldus wordt opgevangen niet aan derden mag worden doorgegeven**. Evenmin is het als een inbreuk op het telefoongeheim te beschouwen wanneer ten behoeve van de opsporing van zgn. telefoonplagers wordt geregistreerd tussen welke aansluitingen en op welke tijdstippen een verbinding tot stand werd gebracht, **zolang van de inhoud van het gesprek niet wordt kennis genomen**.

(…) De telegrafie is niet meer beperkt tot de traditionele vorm van de open aangeboden berichten. Het hele netwerk van telexverbindingen valt er thans onder en deze communicatievorm functioneert veelal automatisch, hetgeen wil zeggen dat er van verzender tot ontvanger geen sprake behoeft te zijn van enige menselijke tussenkomst. De overheid is daar **niet meer gedwongen om van de inhoud van de verzonden berichten kennis te nemen**. Maar ook bij de open aangeboden berichten is het telegraafgeheim niet zonder betekenis in verband met het bovenvermelde feit, dat de **ambtenaar, die** het bericht ontvangt en **van de inhoud kennis neemt, tot geheimhouding verplicht is, welke geheimhoudingsplicht in beginsel ook tegenover andere overheidsfunctionarissen geldt**.' [12]

'Ten slotte zij opgemerkt, dat het telefoon- en telegraafgeheim alleen dan onschendbaar kan zijn wanneer degene, die zich van deze media bedient, er zijnerzijds zorg voor draagt dat van een geheim te houden communicatie sprake kan zijn. Wie een telefoongesprek voert met gebruikmaking van een ontvanginrichting voor **draadloze telefonie, zodat een ieder, die over een zodanige inrichting beschikt, het gesprek kan opvangen**, kan zich **niet op het grondrecht beroepen**.'[13]

Het gemeenschappelijke kenmerk bij alle communicatievormen is dat het bij het correspondentiegeheim gaat om het kennisnemen van de inhoud van de communicatie door de transporteur. Er bestaat een karakterverschil tussen brief, telefoongesprek en telegram, aangezien bij de transporteur bij de brief nooit, bij het telefoongesprek soms (voor technische controle) en bij het telegram meestal (behalve bij telex) kennis moet nemen van (een deel van) de inhoud om het bericht te kunnen transporteren. Maar ook wanneer de transporteur uit de aard der zaak kennis neemt van de inhoud van een bericht, geldt het correspondentiegeheim, in die zin dat de transporteur de inhoud niet mag doorvertellen aan derden.

Van Dorst verheldert deze reikwijdte door een onderscheid te maken tussen het postgeheim in enge zin en het postgeheim in ruime zin.

'De **ratio van het postgeheim in enge zin, t.w. de bescherming van het privé-leven** tegen inbreuk daarop van de zijde van de overheid (…). De technische ontwikkelingen (…) hebben er ook toe geleid dat de telefoon met de brief kan concurreren als middel om **met de buitenwereld contact te onderhouden**, d.w.z. dat de gemiddelde telefoongebruiker **er niet op bedacht** zal zijn – en ook niet **behoeft te zijn – dat anderen kennis nemen van de inhoud** van het gesprek.'[14]

'Naast het postgeheim in enge zin, dat geënt is op de garantie van een "staatsvrije" privésfeer, staat het postgeheim in ruime zin, dat als het ware een uitvloeisel vormt van het eerste en daarmee onverbrekelijk is verbonden en dat zijn grond vindt in **het vertrouwen** dat de burger mag stellen in de functionarissen van de openbare post-, telefoon- en telegraafdienst, **dat dezen de kennis die zij**

[12] *Kamerstukken II* 1975-76, 13 872, nr. 3, p. 44-45.
[13] *Kamerstukken II* 1975-76, 13 872, nr. 3, p. 46
[14] Van Dorst 1982, p. 288.

opdoen bij de uitoefening van hun functie niet aan derden bekend zullen maken. (…) Op grond van deze vertrouwensrelatie behoren de genoemde ambtenaren **geheimhouding** te betrachten **over alles wat zij bij de uitoefening van hun functie te weten komen omtrent post-, telefoon- en telegraafverkeer tussen bepaalde personen** (…).'[15]

Het correspondentiegeheim in ruime zin omvat volgens Van Dorst dus ook verkeersgegevens ('alles (…) omtrent post-, telefoon- en telegraafverkeer'), hoewel dat niet met zoveel woorden te lezen valt in de toelichting van de wetgever. De citaten uit de wetsgeschiedenis omtrent het correspondentiegeheim in ruime zin betreffen immers alleen de kennis die de transporteur in de uitoefening van zijn functie opdoet over de inhoud van de communicatie.

Wetsvoorstel 25443 sloot verkeersgegevens uit omdat zij niet inhoud van communicatie betreffen:

'Verkeersgegevens – daarbij gaat het om gegevens als het feit dat getelefoneerd wordt, met wie en waar – verschillen fundamenteel van het type informatie dat verkregen wordt bij de interceptie van de inhoud van vertrouwelijke communicatie en vallen op grond van hun aard reeds niet onder dit begrip. (…) Het **enkele feit dat verkeersgegevens informatie verschaffen omtrent het communicatieproces**, is **onvoldoende** rechtvaardiging om aan dit type gegevens hetzelfde niveau van **grondwettelijke bescherming** te geven als **aan de communicatieinhoud** zelf.'[16]

Vervolgens nam de Tweede Kamer een amendement aan waarmee ook verkeersgegevens binnen de reikwijdte van artikel 13 Gw werden gebracht: naast het correspondentiegeheim zelf bevatte artikel 13 lid 1 ook 'het geheim van de gegevens met betrekking tot communicatie als bedoeld in de eerste volzin'.[17] Dit werd niet gemotiveerd in het amendement en de behandeling in de Tweede Kamer beperkte zich tot algemeenheden als: 'Verkeersgegevens zijn onzes inziens een intrinsiek onderdeel van de vertrouwelijkheid van communicatie en zouden dus onder artikel 13 moeten vallen.'[18] De Eerste Kamer had echter grote moeite met het wetsvoorstel (hoewel niet primair vanwege het opnemen van verkeersgegevens[19]); het wetsvoorstel werd daarom ingetrokken.[20]

De Commissie-Franken sloot zich aan bij de redenering uit wetsvoorstel 25 443:

'De Commissie is van mening dat **onvoldoende rechtvaardiging** bestaat om onderscheid aan te brengen in het grondwettelijke beschermingsniveau tussen categorieën persoonsgegevens op grond van het feit dat **zij gerelateerd zijn aan een inhoud** die zelfstandig grondwettelijke bescherming geniet.'[21]

Het gaat volgens de commissie dus om de inhoud zelf en niet om aan de inhoud gerelateerde gegevens. Dit werd overgenomen in een in 2004 gepubliceerd concept-wetsvoorstel ter actualisering van artikel 13 Gw, die de volgende toelichting gaf over de ratio en reikwijdte:

'**Vertrouwelijkheid van communicatie** vormt in een democratische rechtsstaat een zwaarwegend belang. Door de kwetsbaarheid van communicatie vormt een inbreuk op vertrouwelijke communicatie in de ogen van de regering een ernstige schending van de persoonlijke levenssfeer van betrokkenen, die een specifieke hoge mate van bescherming rechtvaardigt. (…) Anders dan hetgeen de Registratiekamer aangeeft in het rapport "Grondrechten in het digitale tijdperk", bestaat naar de mening van de regering onvoldoende rechtvaardiging om verkeersgegevens onder de specifieke bescherming van artikel 13 te brengen. Deze conclusie hangt samen met het feit dat **verkeersgegevens weliswaar in de informatiesamenleving veel over personen kunnen zeggen**, maar dat datzelfde geldt voor veel meer gevoelige gegevens, die ook niet onder de werking van artikel 13 vallen. De **inhoud van vertrouwelijke communicatie** is onder een, ook door de Tweede Kamer gewenst, **hoog beschermingsregime** gebracht: voor een beperking is een rechterlijke last vereist. Er zijn **geen goede argumenten** aan te voeren om een onderscheid aan te brengen in het grondwettelijke beschermingsniveau tussen categorieën persoonsgegevens **op grond van het feit**

[15] Ibid., p. 289.
[16] *Kamerstukken II* 1996-97, 25 443, nr. 3, p. 3-4.
[17] *Kamerstukken II* 1997-98, 25 443, nr. 13.
[18] *Handelingen II* 14 januari 1998, 41-3351.
[19] Asscher 2000.
[20] *Kamerstukken II* 1998-1999, 25 443, nr. 40d.
[21] Commissie Grondrechten in het digitale tijdperk 2000, p. 160.

dat zij al dan niet gerelateerd zijn aan een inhoud die zelfstandig grondwettelijke bescherming geniet.' [22]

De Raad van State kon zich in dit onderdeel vinden, maar drong aan op een nadere toelichting:

'De Raad kan zich verenigen met de opvatting dat verkeersgegevens niet dienen te worden beschouwd als bestanddeel van de door artikel 13 beschermde vertrouwelijke communicatie. (…) De kernvraag moet zijn of voor het beschermen van verkeersgegevens behoefte bestaat aan een soortgelijk met extra waarborgen omgeven regime. **De strekking van artikel 13 is dat burgers zonder inmenging vertrouwelijk met elkaar kunnen communiceren.** Zou iemand weten of vermoeden dat **de overheid weet welke telefoongesprekken hij voert**, dan zou dat voor hem reden kunnen zijn om bepaalde gesprekken niet meer te voeren. Dit **doorbreekt de vertrouwelijkheid van de communicatie op zichzelf niet, maar raakt wel de vrijheid van (tele)communicatie**. De Raad adviseert de toelichting op de nu gemaakte keuze om de bijzondere bescherming van artikel 13 geen betrekking te laten hebben op verkeersgegevens, te verbeteren.'[23]

Hoewel niet helemaal duidelijk is wat hier bedoeld wordt, lijkt de Raad te vragen om een scherper onderscheid tussen de vertrouwelijkheid van communicatie (waarop verkeersgegevens geen inbreuk maken) en het recht of de vrijheid om vertrouwelijk te kunnen communiceren (waarop verkeersgegevens, in de zin van 'welke telefoongesprekken' iemand voert, wel inbreuk maken). Vermoedelijk komt dat overeen met het onderscheid tussen het correspondentiegeheim in enge zin (vertrouwelijkheid van communicatie als zodanig) en in ruime zin (het vertrouwelijk kunnen communiceren). De Raad van State laat de mogelijkheid open dat dit laatste ook door artikel 13 beschermd wordt, naast de bescherming van vertrouwelijke communicatie als zodanig.

Het wetsontwerp-2012 grondt in navolging van de commissie-Thomassen artikel 13 Gw op het belang van privé-communicatie:

'De Staatscommissie Grondwet omschreef het belang van de bescherming van privé-communicatie als "men moet in een democratische samenleving **vertrouwelijk met elkaar kunnen communiceren, zonder de angst dat de overheid meeluistert**."[24] Deze invulling van **het rechtens te beschermen belang**, dat schuilgaat achter het huidige artikel 13, sluit in onze optiek naadloos aan bij het rechtens te beschermen belang achter het brief- en telecommunicatiegeheim in onderhavig wetsvoorstel. Met privé-communicatie wordt bedoeld communicatie die niet voor het publiek toegankelijk is, anders dan door de verzender aangewezen. (…) De privé-communicatie wordt specifiek beschermd door artikel 13 en wordt separaat beschermd **omdat de inhoud van de communicatie privé behoort te blijven**. (…) Burgers kunnen immers alleen dan privé communiceren indien zij **niet bevreesd hoeven zijn voor heimelijke inzage door derden die zijn betrokken bij de overdracht of de opslag van de inhoud van de communicatie**.'[25]

De nadruk ligt hier wederom op de vertrouwelijkheid van communicatie: artikel 13 Gw beschermt tegen kennisneming van de inhoud, zowel door de communicatieaanbieder als door de overheid in brede zin.

Dat artikel 13 Gw beschermt tegen kennisneming van de inhoud van communicatie, blijkt ook uit de formuleringen waarmee de wetgever het correspondentiegeheim in wetgeving heeft vormgegeven. Bij post gaat het om het openen (en, naar men mag aannemen, vervolgens lezen) van brieven, blijkens onder andere artikel 23 Wiv 2002 ('De diensten zijn bevoegd tot het openen van brieven en andere geadresseerde zendingen') en artikel 101 Sv ('kennisneming van de inhoud der' 'inbeslaggenomen pakketten, brieven, stukken en andere berichten'). Bij telecommunicatie gaat het om het opnemen (en afluisteren) van telecommunicatie, aldus onder andere artikel 25 Wiv 2002 en artikel 126m/t/zg Sv, alsmede om het opvragen van 'gegevens die zijn opgeslagen in het geautomatiseerde werk van de aanbieder en niet voor deze bestemd of van deze afkomstig zijn' (art. 126ng/ug/zo Sv), waarmee de inhoud van bij de communicatieaanbieder opgeslagen email of stempost wordt bedoeld.

[22] Voorstel van wet, bijlage bij Brief van de Minister van Bestuurlijke Vernieuwing en Koninkrijksrelaties aan de Koningin, 29 oktober 2004, kenmerk 0000018194, p. 5, 10.
[23] Advies Raad van State 24 januari 2002, bijgevoegd bij Brief van de Minister van Bestuurlijke Vernieuwing en Koninkrijksrelaties aan de Koningin 29 oktober 2004, kenmerk 0000018194, p. 6-7.
[24] Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, 2010, p. 85.
[25] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 9-10.

Samenvattend: in de loop van de geschiedenis is de grondwetgever ervan uitgegaan dat artikel 13 Gw beschermt tegen kennisneming van de inhoud van communicatie door de transporteur, en in het verlengde daarvan de overheid (strafvordering of veiligheidsdiensten) die via de transporteur de inhoud zou kunnen vorderen; dit is het correspondentiegeheim in enge zin. Artikel 13 Gw biedt ook bescherming wanneer het inherent is aan het transport dat de transporteur kennis neemt van (een deel van) de inhoud van communicatie, de transporteur mag de inhoud dan niet doorvertellen aan derden; dit is het correspondentiegeheim in ruime zin. Van oudsher vallen verkeersgegevens volgens de grondwetgever niet onder de reikwijdte van artikel 13 Gw; bij de herzieningsvoorstellen in de afgelopen jaren is die lijn grotendeels doorgetrokken: het correspondentiegeheim beschermt tegen kennisname van de inhoud maar niet tegen kennisname van het communicatieproces.

2.2. Literatuur

Sinds Van Dorst in 1982 opmerkte dat de wetgever nergens een beschouwing had gegeven over de grondslag van het postgeheim,[26] heeft de wetgever wel indicaties gegeven van de ratio van het correspondentiegeheim, maar een scherp of consistent beeld schetst daarvan valt niet op te maken uit de wetsgeschiedenis. In de wijzigingsvoorstellen van de afgelopen decennia worden wisselende formuleringen gehanteerd die niet precies dezelfde grondslag voor beschermwaardigheid kennen: het belang van vertrouwelijke communicatie, het belang van vertrouwelijkheid van communicatie of het belang vertrouwelijk te kunnen communiceren. De focus op bescherming tegen kennisneming van de inhoud door de transporteur en/of overheid suggereert dat de vertrouwelijkheid van communicatie voorop staat, dat wil zeggen de vertrouwelijkheid van datgene wat wordt gecommuniceerd. Tegelijkertijd vallen in de commissierapporten en wetsvoorstellen van de afgelopen decennia ook de nodige uitspraken te lezen die het correspondentiegeheim plaatsen in de context van het belang om vertrouwelijk te kunnen communiceren of het belang van vertrouwelijke of privé-communicatie; bij die ratio past eerder dat de vertrouwelijkheid van het communicatieproces wordt beschermd, oftewel niet alleen datgene wat er wordt gecommuniceerd maar ook dat en hoe er wordt gecommuniceerd.

In de literatuur waarin gepoogd wordt het correspondentiegeheim te duiden, veelal afkomstig van de Amsterdamse school, is deze laatste benadering dominant. Hoewel er verschillende accenten voorkomen in de benadering van het correspondentiegeheim, gaan de auteurs er vrijwel steeds van uit dat de ratio van bescherming vooral gelegen is in de bescherming van het communicatieproces als geheel. In die benadering vallen ook verkeersgegevens onder de reikwijdte van de bescherming.

Volgens Hofman wordt niet alleen de communicatievorm, maar ook het communicatieproces beschermd door artikel 13 Gw.[27] Hij vindt daarvoor steun in de interpretatie die het Europees Hof van de Rechten de Mens heeft gegeven aan het begrip 'correspondence' uit artikel 8 EVRM: 'niet alleen het afluisteren van de inhoud is verboden, maar evenzeer het verzamelen van verkeersgegevens, die een "integral element" vormen van de communicatie per telefoon'.[28] Deze geïntegreerde benadering wordt op Europees niveau breed gedeeld, bijvoorbeeld door de Artikel 29 Werkgroep:

> 'The Article 29 Working Party has dealt with the privacy aspects of interception of communications in its recommendation 2/9956. In this recommendation, the Working Party points out that each interception of telecommunications, defined as a third party acquiring knowledge of the **content and/or traffic data** relating to private telecommunications between two or more correspondents, and in particular of traffic data concerning the use of telecommunications services, **constitutes a violation** of an individual's right to privacy and **of the confidentiality of correspondence**.'[29]

Volgens Dommering beschermt het correspondentiegeheim het kanaal als geheel:

> 'waar het om draait: het brief- en telefoongeheim beschermen de verzender van een boodschap tegen de kennisneming van de inhoud daarvan door degene die met de verzending is belast, of tegen degenen die via de transporteur toegang tot de verzonden boodschap zouden kunnen hebben. Het gaat daarbij niet om de inhoud van de boodschap. Deze kan strikt geheim zijn (een

[26] Zie noot 5.
[27] Hofman 1995, p. 149 en 462.
[28] Ibid., p. 103, verwijzend naar EHRM 2 augustus 1984, *Malone t. Verenigd Koninkrijk*, App.no. 8691/79.
[29] Article 29 Working Party 2000, p. 35.

bedrijfsgeheim, een liefdesverklaring), maar ook juist bestemd zijn om openbaar te worden gemaakt (een artikel, een ingezonden brief). Het gaat om de vertrouwelijkheid van het communicatie*kanaal*: het brief- en postgeheim zijn in hun essentie klassieke onthoudingsrechten, die op de beheerders van netten en aanbieders van informatietransportdiensten de plicht leggen **zich te onthouden van een inmenging in de verzonden boodschap**.'[30]

In deze benadering ziet de bescherming

'niet alleen op de inhoud van de boodschap, maar ook op de adresseergegevens, ook wel aangeduid als "verkeersgegevens". Het waarnemen en opslaan van gegevens (bij elektronische communicatie regel) vormt mede een inbreuk op het recht.'[31]

'Het gaat bovendien niet alleen om verkeersgegevens. Ik noem de adressering op de enveloppe, inloggegevens omtrent de verzending en het ophalen van e-mail berichten, naar de identiteit van de opgebelde gespecificeerde telefoonrekeningen en andere uitsluitend door het transport gegenereerde persoonsgegevens. Ik zou ze alle willen toerekenen aan het transportgeheim. Naar analogie van het Duitse recht zou men kunnen spreken van het *Auskunftverbot* (als pendant van het *Eindringeverbot*), het verbod feiten mee te delen over de omstandigheden van verzending. Hetgeen betekent dat ze alleen binnen de beperkingen van het transportgeheim aan derden kunnen worden verstrekt.'[32]

De ratio hiervan wordt goed verwoord door Asscher:

'Terwijl artikel 10 Grondwet ziet op de bescherming van de persoonlijke levenssfeer, ziet het transportgeheim op **de betrouwbaarheid van het communicatiekanaal**. Geheimhouding van verkeersgegevens dient deze betrouwbaarheid. Het gaat er dan ook niet zo zeer om dat verkeersgegevens veel over personen kunnen zeggen, belangrijker is dat **het vertrouwen dat de burger stelt in het communicatiekanaal** kan worden aangetast, wanneer verkeersgegevens worden verwerkt voor **doelen die niet noodzakelijkerwijs voortvloeien uit het leveren van deze dienst**. Wanneer de burger er rekening mee moet houden dat wordt bijgehouden met wie hij wanneer en hoe lang communiceert en vervolgens deze informatie buiten het kader van de dienst voor allerlei doeleinden wordt verwerkt, zal hij niet meer **vrij kunnen communiceren**.'[33]

Dit sluit aan bij de visie die Van Dorst al in 1982 formuleerde op het correspondentiegeheim in ruime zin:

'Eigenlijk zou de grens al eerder, dus nog vóór het bekend maken van ambtelijk verkregen informatie, getrokken moeten worden, in dier voege dat het de ambtenaar verboden zou dienen te zijn van meer kennis te nemen dan voor de richtige vervulling van de hem opgedragen taak noodzakelijk is. (…) De bescherming die de burger aldus – op indirecte wijze – wordt geboden heeft dus **niet zozeer de geheimhouding van de inhoud** van de door hem gevoerde correspondentie ten doel, **maar meer de geheimhouding van alle feiten die noodzakelijkerwijs samenhangen met of noodzakelijkerwijs voortvloeien uit het gebruik van openbare diensten**. Te denken valt in dit verband aan informatie met betrekking tot de vraag of iemand met een ander in contact staat, met wie, waarover, etc., welke gegevens voor de vraagsteller zeer onthullend zouden kunnen zijn.'[34]

Volgens Steenbruggen is de ratio van het correspondentiegeheim dat het

'als een vooruitgeschoven **verdedigingslinie voor zowel het recht op privacy als de communicatievrijheid** functioneert. Als zodanig beschermt het grondrecht de vertrouwelijkheid van persoonlijke communicatie. (…) Bijkomende ratio is dat de burger ervan uit moeten [sic] kunnen gaan dat hij zijn **communicatie *veilig*** aan een aanbieder van openbare post en telecommunicatiediensten **kan toevertrouwen**.'[35]

In deze literatuur wordt aldus een visie op het correspondentiegeheim neergezet waarin de ratio van bescherming is gelegen in de vrijheid om vertrouwelijk te kunnen communiceren. Gegeven die ratio ligt het voor de hand de reikwijdte van het correspondentiegeheim zich te laten uitstrekken over het communicatieproces als geheel. Het correspondentiegeheim – in ruime zin – omvat dan ook verkeersgegevens, omdat kennisneming van het communicatieproces door de

[30] Dommering 1997, p. 117.
[31] Dommering 2000, p. 72.
[32] Dommering 1997. In vergelijkbare zin: Studiecommissie VMC 1999, p. 6-7.
[33] Asscher 2003, p. 24.
[34] Van Dorst 1982, p. 290.
[35] Steenbruggen 2009, p. 69.

overheid via de transporteur een inbreuk maakt op de vrijheid om vertrouwelijk te kunnen communiceren.

2.3. Afbakening van het begrip 'inhoud'

Hoewel de dominante visie in de literatuur een bredere reikwijdte hanteert dan de wetgever door ook verkeersgegevens onder de bescherming van het correspondentiegeheim te brengen, lost deze benadering het probleem van de afbakening van inhoud tegenover verkeersgegevens niet op. Het feit dat verkeersgegevens onder het correspondentiegeheim (zouden moeten) vallen, wil namelijk niet zeggen dat ze op dezelfde wijze beschermd moeten worden als inhoud.[36] Zoals de wetgever van 1983 heeft erkend dat er een karakterverschil bestaat tussen communicatievormen naar gelang het meer of minder vanzelfsprekend is dat de transporteur ter uitvoering van het transport kennis neemt van de inhoud, zo bestaat er een karakterverschil tussen het correspondentiegeheim in enge zin (dat een sterke werking heeft) en het correspondentiegeheim in ruime zin (dat een zwakkere werking heeft). Dat karakterverschil komt goed tot uiting in het historische gegeven dat de strafvorderlijke bevoegdheid tot het opvragen van verkeersgegevens aanvankelijk ook inhoud van telefoongesprekken omvatte, voor zover de telefoonoperator daarvan kennis had genomen bij het doorverbinden van het gesprek.[37] Met de automatisering van de telefonie was er geen operationele reden meer voor de operator om mee te luisteren (behalve het incidenteel inluisteren voor technische controle), waardoor de inhoud een vertrouwelijker karakter kreeg en verschoof naar het correspondentiegeheim in enge zin. Dit geeft aan dat er een afbakening nodig is, wellicht niet zozeer tussen inhoud en verkeersgegevens, maar vooral tussen gegevens waarvan de transporteur niet uit de aard van zijn functie kennis hoeft te nemen (waarvoor het sterkere correspondentiegeheim in enge zin geldt) en gegevens waarbij dat wel het geval is (waarvoor het zwakkere correspondentiegeheim in ruime zin geldt). In het huidige communicatielandschap heeft dit onderscheid een sterke parallel met het onderscheid tussen inhoud en verkeersgegevens.

Aangezien zowel wetgever als de literatuur hoofdzakelijk een onderscheid maken tussen inhoud en verkeersgegevens, waarbij in elk geval de inhoud van communicatie op een sterke bescherming kan rekenen en open gelaten wordt welke bescherming de verkeersgegevens zouden moeten krijgen, rijst de vraag wat nu precies onder inhoud valt. Hierover valt geen expliciete uitspraak te vinden in wetsgeschiedenis of literatuur. Indirecte aanknopingspunten kunnen worden gevonden in de precieze formulering die auteurs gebruiken om aan te duiden wat wel en niet onder 'inhoud' valt.

MacGillavry omschrijft inhoudelijke gegevens als 'gegevens die inzicht geven in de werkelijke inhoud van de communicatie'.[38] Hij omschrijft echter niet wat 'de werkelijke inhoud is'; mogelijk gaat het om de letterlijke inhoud van het bericht, maar mogelijk ook om de hermeneutische inhoud van de boodschap. Verkeersgegevens omschrijft hij als gegevens die informatie geven over het gebruik van de diensten van de ISP door de gebruiker.[39] De Commissie-Franken geeft evenmin een omschrijving van inhoud; zij stelt dat verkeersgegevens geen betrekking hebben op de inhoud van het gegevensverkeer maar dat zij 'gerelateerd zijn aan een inhoud die zelfstandig grondwettelijke bescherming geniet.'[40] Dit betekent dat verkeersgegevens niet zelf inhoud zijn maar in een zekere verhouding staan tot inhoud. Dat zou kunnen betekenen dat gegevens die een zeker inzicht geven in de inhoud maar niet letterlijk zelf tot de inhoud behoren, onder

[36] Vgl. bijvoorbeeld ibid., p. 56-57: 'Gelet op het bovenstaande zijn er goede gronden om de bescherming van verkeersgegevens en de bescherming van de inhoud van communicatie ineen te schuiven. (…) Dat betekent niet per definitie dat verkeersgegevens in alle gevallen dezelfde bescherming als de inhoud van communicatie moeten krijgen.'

[37] Een instructie bij de dienstorder van 29 december 1925 die diende om de bepalingen uit het nieuwe Wetboek van Strafvordering aan de ambtenaren der PTT ter kennis te brengen, gaf het volgende aan: 'De ambtenaren zijn eveneens verplicht aan den Officier van Justitie op diens vordering op grond van bovengenoemd artikel van het W. Sv. [art. 100, het latere art. 125f en huidige art. 126n, bjk] de door deze gewenschte inlichtingen te verstrekken terzake van alle telefonisch verkeer (*dus ook omtrent den inhoud der telefoongesprekken*, voor zoover de ambtenaar daarvan zonder schending van de ambtsplicht heeft kunnen kennis nemen)' (cursivering toegevoegd). INSTRUCTIE, behoorend bij dienstorder no. 831 van 29 December 1925 van het Hoofdbestuur der Posterijen en Telegrafie. Zie hierover Koops 2002, p. 118-119.

[38] MacGillavry 2004, p. 231.

[39] Ibid., p. 225.

[40] Commissie Grondrechten in het digitale tijdperk 2000, p. 160.

verkeersgegevens en niet onder inhoud vallen; de formulering kan echter ook simpelweg een meer technische aanduiding zijn van verkeersgegevens als zijnde meta-gegevens, zonder iets te zeggen over het feit of verkeersgegevens al dan niet samenhangen of tot op zekere hoogte samenvallen met inhoud.

Het wetsontwerp-2012 is iets explicieter in dit opzicht. Het ontwerp maakt een onderscheid tussen de technische kwalificatie en de juridische kwalificatie:

> 'De inhoud van de communicatie is overigens nog te onderscheiden van de **gegevens die worden gegenereerd** met betrekking tot de totstandkoming, de duur en het tijdstip van de communicatie. Deze gegevens worden hierna geduid als verkeersgegevens (…) Deze gegevens behoren niet primair tot het belang dat artikel 13 beoogt te beschermen, omdat zij **niet de inhoud van het bericht weergeven**. Niet kan worden uitgesloten dat zij daarvan **wel deel uitmaken indien zij nauw verband houden met de inhoud** van het bericht.'[41]

> 'Aandacht verdient evenwel dat de inhoud van telecommunicatie in technische zin soms ook als een verkeersgegeven wordt gezien. Zo wordt het onderwerp van een e-mail in technische zin wel tot de verkeersgegevens betreffende die e-mail gerekend. Maar in juridische zin valt het onderwerp van een e-mail onder de reikwijdte van artikel 13 omdat dat onderwerp **betrekking heeft op de inhoud** van de e-mail. Een ander voorbeeld is een sms-bericht: technisch gezien is een dergelijk bericht in zijn geheel een verkeersgegeven, maar juridische gezien omvat een sms-bericht – naast verkeersgegevens – tevens de inhoud van communicatie. De conclusie is dat aan de bescherming van artikel 13 niet kan afdoen dat gegevens die de inhoud van communicatie betreffen in technische zin als een verkeersgegeven worden beschouwd. **Verkeersgegevens die niet mede betrekking hebben op de inhoud van telecommunicatie vallen echter buiten de reikwijdte** van artikel 13.'[42]

> 'Ook voor verkeersgegevens die geheel of ten dele mede betrekking hebben op de inhoud van de communicatie, zoals de onderwerpregel van een e-mail en de in een internetzoekmachine ingevoerde zoekterm (…), geldt dat deze slechts [met rechterlijke machtiging] mogen worden gevorderd. (…) Als verkeersgegevens zijn krachtens de artikelen 126n, 126u en 126zh Sv (in het Besluit vorderen gegevens telecommunicatie) alleen **gegevens** aangewezen **die niet geheel of ten dele mede op de inhoud van de communicatie betrekking** hebben.'[43]

In deze passages worden drie licht verschillende formuleringen gebruikt voor de afbakening van verkeersgegevens en inhoud. Gegevens vallen onder inhoud als zij 'nauw verband houden met', 'mede betrekking hebben op' dan wel 'geheel of ten dele mede betrekking hebben op' de inhoud van communicatie. Het laatste criterium sluit aan bij de afbakening die Koops in 2003 maakte in de strafvorderlijke bevoegdheden:

> 'Een goed uitgangspunt hierbij is dat indien gegevens worden opgevraagd **die deels (hoe weinig ook) inhoud** van telecommunicatie **betreffen**, deze moeten vallen onder de telecomtap en niet onder de bevoegdheid van verkeersgegevens.'[44]

Deze formulering is potentieel zowel ruimer als beperkter dan die in wetsontwerp-2012. Het biedt een zo ruim mogelijke reikwijdte van de inhoud, door te expliciteren dat zodra gegevens ook maar enig deel van de inhoud betreffen, deze onder de bescherming van inhoud vallen; het wetsontwerp-2012 kan op deze manier worden geïnterpreteerd, maar laat ook de mogelijkheid open dat gegevens ten minste voor een substantieel deel de inhoud moeten betreffen. Aan de andere kant is de formulering van Koops wat beperkter omdat het gaat om verkeersgegevens die inhoud 'betreffen', terwijl het wetsontwerp spreekt van gegevens die 'betrekking hebben op' inhoud. Hoewel de begrippen nauw verwant zijn, lijkt mij 'betreffen' een directere relatie aan te duiden dan 'betrekking hebben op'. In die lezing lijkt de formulering van Koops beperkt tot verkeersgegevens die zelf onderdeel uitmaken van de inhoud, terwijl de formulering van wetsontwerp-2012 de interpretatiemogelijkheid biedt om ook verkeersgegevens onder inhoud te laten vallen als zij een aanduiding geven van de (globale) inhoud maar niet zelf, letterlijk, deel uitmaken van de inhoud. Dit interpretatieverschil geeft aan dat het nodig is om meer greep te krijgen op wat precies het nauwe verband moet zijn van verkeersgegevens met inhoud om ze

[41] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 12.
[42] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 17-18.
[43] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 32. Vgl. ook het criterium zoals Steenbruggen 2009, p. 337 het formuleert in zijn voorstel voor een nieuw art. 13 Gw: verkeersgegevens worden als inhoud beschermd als zij '**mede betrekking hebben op de inhoud van de communicatie**'.
[44] Koops 2003, p. 69.

onder de bescherming van inhoud te brengen, maar ook op wat dan precies de 'inhoud zelf' is van een bericht waartoe verkeersgegevens in dat nauwe verband staan.

Fischer is de enige die een poging gedaan heeft een materiële omschrijving te geven van wat de inhoud van communicatie is. Hij definieert inhoud (*content data*) als:

> 'data for which the intermediary service provider is (conditionally) exempted from liability: data in a state of mere conduit, caching or hosting.'[45]

Dit lijkt op het eerste oog een wat merkwaardige omschrijving van het begrip 'inhoud van communicatie', omdat het is ontleend aan een juridische formulering betreffende de aansprakelijkheid van Internetaanbieders. De achterliggende gedachte van de aansprakelijkheidsuitsluiting is dat Internetaanbieders over het algemeen niet aansprakelijk zijn voor de inhoud van communicatie van hun gebruikers, tenzij zij zich die inhoud hebben eigen gemaakt en er daardoor mede verantwoordelijk voor zijn geworden. Dit biedt daarom een interessant aanknopingspunt voor het antwoord op de vraag wat onder 'inhoud' van communicatie moet worden volstaan: inhoud is datgene waarvoor de transporteur (in zijn rol van transporteur)[46] niet verantwoordelijk is. Of positief geformuleerd: inhoud is datgene wat valt onder de verantwoordelijkheid van de verzender.

Op deze manier kan inhoud functioneel worden afgebakend ten opzichte van verkeersgegevens, die dan gegevens zijn die wel vallen onder de verantwoordelijkheid van de transporteur. Dit zijn gegevens 'die betrekking hebben op de overdracht of op de opslag van het bericht'[47] of 'inlichtingen omtrent de wijze van totstandkoming en afwikkeling van het telecommunicatieverkeer'.[48] Ze worden ook wel aangeduid als 'inhoudloze transmissiegegevens'[49] of 'verbindingsgegevens'[50]. Een kernkarakteristiek van verkeersgegevens is dat de communicatiedeelnemer alleen invloed kan uitoefenen op het verkeersgegeven door haar communicatiegedrag aan te passen (bijvoorbeeld door een bepaald nummer niet te bellen, of op een ander tijdstip), maar geen controle heeft over de uiteindelijke inhoud van de verkeersgegevens.[51] Dit sluit goed aan bij de conceptualisering van Fischer dat inhoud onder de verantwoordelijkheid van de communicatiedeelnemer valt, omdat zij daar controle over kan uitoefenen.

Bepaalde omschrijvingen van verkeersgegevens leggen de nadruk op het feit dat de verkeersgegevens niet afkomstig zijn van de verzender maar door de transporteur zelf worden gegenereerd:

> 'de **gegevens die worden gegenereerd** met betrekking tot de totstandkoming, de duur en het tijdstip van de communicatie'.[52]

> '"verkeersgegevens" [zijn] computergegevens die verband houden met een met behulp van een computersysteem gevoerde communicatie, en **worden voortgebracht door een computersysteem** dat een onderdeel vormt van de communicatieketen, en de herkomst, de bestemming, de route, de tijd, de datum, de omvang, de duur of de aard van de betrokken dienst aanduiden.'[53]

De telecommunicatiewetgeving hanteert een wat ruimere definitie dan transportgegevens door ook gegevens die nodig zijn voor facturering onder de definitie te laten vallen: 'gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan'.[54] In meer algemene zin kunnen verkeersgegevens daarom ook worden omschreven als

---

[45] Fischer 2010, p. 29-30.
[46] Vgl. art. 54a Sr: 'Een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt *als zodanig* niet vervolgd indien (…)'; de woorden 'als zodanig' betekenen dat hij onder bepaalde voorwaarden niet vervolgd wordt *als tussenpersoon*, maar mogelijk wel als (mede-)inhoudsaanbieder.
[47] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 16.
[48] HR 7 september 2004, LJN AO9090.
[49] Smits 2006, p. 4.
[50] Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, 2010, p. 89.
[51] Smits 2006, p. 404n.
[52] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 12.
[53] Art. 1(d) Cybercrime-Verdrag.
[54] Art. 2(b) Richtlijn 2002/58/EG.

‘alle feiten die noodzakelijkerwijs samenhangen met of noodzakelijkerwijs voortvloeien uit het gebruik van openbare [post- of telecommunicatie]diensten’.[55]

Voor een functionele specificering van welke gegevens noodzakelijk zijn voor de transporteur om zijn dienst te kunnen leveren, biedt Fischer een nuttig raamwerk. Fischer definieert verkeersgegevens aanvankelijk als ‘data just processed for the provider’s good reasons’,[56] wat hij vervolgens nader uitwerkt in een preciezere definitie:

‘Traffic data: electronic personal data on the actual use of the network **processed by intermediary service providers for three essential functions in three types of services**.

The essential data processing functions of the intermediary service provider are:

1. service performance: data processing to carry out the service agreement with the user;

2. service accounting: data processing for billing and verification of the service;

3. service management: data processing for traffic management and network maintenance.

The three types of services of the intermediary service provider are:

1. mere conduit: the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network;

2. caching: the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service upon their request;

3. hosting: the storage of information provided by a recipient of the service.’[57]

Volgens Fischer biedt dit een bruikbare juridische conceptualisering van het begrip verkeersgegevens, die het mogelijk maakt dit begrip te operationaliseren in de technische werkelijkheid. Om te bepalen of een gegeven een verkeersgegeven is, kan Fischer’s 3x3-test worden uitgevoerd: als het gegeven wordt verwerkt voor een van de drie essentiële functies van een van de drie typen dienstaanbieders, kan het worden gekwalificeerd als verkeersgegeven. Een waterdichte afbakening met inhoud biedt dat niet, omdat het denkbaar is dat bepaalde gegevens in de 3x3-matrix vallen maar ook onder Fischer’s definitie van inhoud, bijvoorbeeld als een webmailaanbieder een bericht opslaat terwijl iemand hem genotificeerd heeft dat de onderwerpsregel daarvan strafrechtelijk beledigend (art. 266 Sr) voor de ontvanger is.

2.4. Conclusie

Het correspondentiegeheim bestaat uit een kern – het correspondentiegeheim in enge zin – die beschermt tegen kennisneming door de transporteur van communicatie (en door derden via hem) van de inhoud van communicatie. Het correspondentiegeheim kent tevens een periferie – het correspondentiegeheim in ruime zin – die beschermt tegen doorvertellen door de transporteur aan derden van kennis over (de inhoud van) communicatie waarvan hij voor de uitoefening van het transport kennis heeft genomen. Of het correspondentiegeheim in ruime zin ook beschermd wordt of zou moeten worden door artikel 13 Gw is niet eenduidig te bepalen. De wetgever heeft in de wetsgeschiedenis en de wijzigingsvoorstellen van de laatste jaren de nadruk gelegd op kennisneming van de inhoud van communicatie; artikel 13 Gw beschermt in die visie niet de vertrouwelijkheid van het communicatieproces maar alleen de vertrouwelijkheid van de inhoud van de communicatie die via een communicatiekanaal wordt getransporteerd. In de literatuur over de ratio van artikel 13 Gw domineert de visie dat dit artikel de vertrouwelijkheid van het communicatieproces beschermt, en daarmee de vrijheid om privé te kunnen communiceren; het correspondentiegeheim beschermt dan ook de gegevens die samenhangen met dat proces (wat overigens niet wil zeggen dat verkeersgegevens aanspraak zouden moeten maken op hetzelfde beschermingsniveau als inhoud). De wetgever lijkt deze laatste interpretatie niet te willen omarmen, hoewel diverse uitspraken over de ratio van het correspondentiegeheim wel spreken

[55] Van Dorst 1982, p. 290. In vergelijkbare zin Asscher 2003, p. 24, die spreekt over een inbreuk op het correspondentiegeheim wanneer ‘verkeersgegevens worden verwerkt voor **doelen die niet noodzakelijkerwijs voortvloeien uit het leveren van deze dienst**.’
[56] Fischer 2010, p. 23.
[57] Ibid., p. 30.

van de behoefte om de vrijheid om vertrouwelijk te kunnen communiceren te beschermen, wat wijst in de richting van bescherming van het gehele communicatieproces. In die zin lijkt er, anders dan in de literatuur van de Amsterdamse school, aan de interpretatie van de wetgever geen systematische visie ten grondslag te liggen over de ratio van het correspondentiegeheim.

Wat daar ook van zij, belangrijk is in elk geval wel dat het correspondentiegeheim in ruime zin onder de reikwijdte van artikel 13 Gw dient te vallen waar het de inhoud van communicatie betreft waarvan de aanbieder ter uitoefening van zijn functie kennis heeft genomen. Zou dat niet zo zijn, dan zou namelijk de grondwetsbepaling niet techniekonafhankelijk zijn; het zou er dan immers van afhangen hoe de aanbieder het communicatieproces inricht of een verzender aanspraak kan maken op het correspondentiegeheim: als de telefonieaanbieder om wat voor reden dan ook zou besluiten terug te gaan naar een schakelcentrale met een telefoonjuffrouw (zodat de operator bij de uitoefening van het transport veelal kennis neemt van de communicatie), zou de grondwettelijke bescherming van het telefoongesprek komen te vervallen. Dat kan niet de bedoeling zijn, nu het nadrukkelijk de intentie is om artikel 13 techniekonafhankelijk vorm te geven.[58] Daarom beschermt artikel 13 Gw de inhoud van communicatie zowel in enge als in ruime zin.

Wat er daarbij onder 'inhoud' van communicatie moet worden verstaan, is niet expliciet af te leiden uit wetsgeschiedenis of literatuur. De enige materiële omschrijving van het begrip 'inhoud' in de literatuur, van Fischer, geeft echter wel een zinvol aanknopingspunt om gegevens te kwalificeren: onder inhoud kan worden verstaan datgene wat onder verantwoordelijkheid van de verzender valt, terwijl verkeersgegevens die gegevens zijn die onder verantwoordelijkheid van de transporteur (als transporteur) vallen. Deze categorieën sluiten elkaar niet volledig uit, maar de omschrijving verheldert wel wat de kern is van inhoud en van verkeersgegevens.

Voor de gevallen waarin er overlap bestaat, is de vraag wanneer verkeersgegevens als inhoud moeten worden behandeld: dat is het geval als zij, geheel of ten dele, (mede) betrekking hebben op de inhoud of (een deel van) de inhoud zelf betreffen. Wat onder 'betrekking hebben op' of 'betreffen' moet worden verstaan, is echter niet duidelijk. Het zou kunnen gaan om gegevens die in letterlijke zin deel uitmaken van de inhoud van de boodschap – dus een deel van de boodschap *zijn* – maar het zou ook kunnen gaan om gegevens die inzicht geven in (een deel van) de boodschap – dus *over* de boodschap *gaan* zonder zelf deel uit te maken van de boodschap.

Een functionele interpretatie van het criterium 'gegevens die (mede) betrekking hebben op de inhoud' zou, gelet op de ratio van bescherming, vermoedelijk meer in de richting van het laatste wijzen. De ratio van het correspondentiegeheim is immers, in de meest recente formulering van de wetgever, dat burgers 'vertrouwelijk met elkaar kunnen communiceren, zonder de angst dat de overheid meeluistert"[59] 'omdat de inhoud van de communicatie privé behoort te blijven.'[60] Het 'meeluisteren' zou, zoals hierboven aangegeven, niet alleen de letterlijke inhoud moeten omvatten, maar ook het doorvertellen van de inhoud door de aanbieder, en bij dit doorvertellen gaat het niet per se om het letterlijk citeren maar om het doorgeven van de (globale) inhoud van het bericht. Ook het doorvertellen van een deel van de inhoud zonder de hele inhoud te onthullen zou onder de bescherming moeten vallen; voor de angst van burgers dat de overheid meeluistert maakt het immers niet principieel uit of de overheid integraal of selectief meeluistert.

Op basis van bovenstaande analyse kan de eerste onderzoeksvraag als volgt worden beantwoord: de 'inhoud' van communicatie is deel van de communicatie dat valt onder de verantwoordelijkheid van de verzender (en niet van de transporteur). Gelet op de ratio van bescherming door artikel 13 Gw vallen hieronder ook gegevens die de strekking weergeven van (een deel van) datgene wat valt onder de verantwoordelijkheid van de verzender.

[58] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 5.
[59] Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, 2010, p. 85.
[60] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 9-10.

3. Grijze gebieden tussen verkeersgegevens en inhoud

In de literatuur alsook in de wijzigingsvoorstellen van de afgelopen jaren wordt regelmatig opgemerkt dat de scheidslijn tussen verkeersgegevens en inhoud soms moeilijk te trekken valt of vervaagt, dan wel dat het onderscheid anderszins aan relevantie verliest.

> 'Een andere belangrijke vraag betreft de huidige en toekomstige status van een aantal specifieke groepen gegevens zoals de 'subject line' van een email of de bezochte webadressen en de omgang met zoekvragen. Hoe je die informatie, die in technische zin tot de verkeersgegevens behoort, maar die in feite veel over de inhoud vertelt, dient te behandelen, is in toenemende mate onduidelijk.'[61]

Bij surfgegevens, zoekvragen en de onderwerpsregel in een emailbericht vervaagt het onderscheid tussen verkeersgegevens en inhoud. Daarnaast wordt ook vaak gewezen op locatiegegevens en de opkomst van *data mining*, die de relevantie van het onderscheid ter discussie stellen. In dit hoofdstuk worden de grijze gebieden tussen verkeersgegevens en inhoud verkend door een overzicht te geven van alle voorbeelden die in de literatuur worden genoemd.

3.1. Surfgegevens

3.1.1. Algemeen

De Artikel 29 Werkgroep geeft aan dat surfgegevens – de gegevens over welke webpagina's iemand heeft bezocht, oftewel de URL's[62] – verkeersgegevens zijn maar als inhoud moeten worden behandeld:

> 'In principle, this Article [artikel 5 van de voorloper van Richtlijn 2002/58/EG over vertrouwelijkheid van communicatie, bjk] refers to the content of the communication. The distinction between traffic data and content is not, however, easy to apply in the context of the Internet, and certainly not when referring to surfing. Surfing data could in principle be regarded as traffic data. However, the Working Party thinks that surfing through different sites should be seen as a form of communication and as such should be covered by the scope of application of Article 5.
>
> The surfing behaviour of an Internet user (navigation data) visiting different websites can in itself reveal a lot about the communication taking place. By knowing the names of the websites visited, one can in most cases gain a fairly accurate picture of the communication which has taken place. Furthermore, it is then **straightforward** for anyone armed with the traffic data **to** visit the site and **see exactly what content was accessed**.
>
> The Working Party thinks, therefore, that the surfing data of an Internet user **should receive the same level of protection as "content"**. This form of communication should therefore remain confidential. In this sense *clickstreams* can be considered as falling within the scope of application of this Article.
>
> The new proposal for a revised directive defines "traffic data" in Article 2.1c): *"traffic data" shall mean any data processed in the course of or for the purpose of the transmission of a communication over an electronic communications network*. Navigation data would therefore fall within this definition and be considered as traffic data.
>
> The revision of this Directive has brought major improvements by extending the scope of Article 5 to cover not just the content of the communication but also the related traffic data. By giving equal protection to content and related traffic data **the (sometimes difficult) distinction between these concepts becomes less important**. The Working Party welcomes this improvement.'[63]

Hoewel de Werkgroep hierin stelt dat surfgegevens zonder meer op het niveau van inhoud moeten worden beschermd, is het rapport niet helemaal consistent; even verderop staat dat

[61] Asscher en Ekker 2003, p. 104.
[62] Zie http://nl.wikipedia.org/wiki/Uniform_Resource_Locator (geraadpleegd 15 januari 2013) en Smits 2013, p. 30.
[63] Article 29 Working Party 2000, p. 50.

surfgegevens *mogelijk* hetzelfde beschermingsniveau moeten krijgen.[64] Ook MacGillavry formuleert het voorzichtig:

> 'Geconstateerd kan worden dat deze gegevens mede informatie over de inhoud van het berichtenverkeer geven. Met deze gegevens kan namelijk de bezochte pagina worden opgeroepen, zodat de inhoud van de bezochte pagina kan worden achterhaald. Om deze reden moeten dergelijke gegevens mogelijk ook als inhoudelijke gegevens worden beschouwd.'[65]

Arno Smits geeft in zijn dissertatie over aftappen en verkeersgegevens een uitgebreide analyse van http-informatie en merkt op dat surfgegevens 'veelal communicatieve elementen bevatten'.[66] Het gaat daarbij echter niet zozeer om het feit dat surfgegevens direct samenhangen met inhoud, maar dat ze veel blootgeven over de interessesfeer, meer dan bij telefoonnummers (bijvoorbeeld als je een pizzeria of een escortservice belt) het geval is. Surfgegevens geven 'veel meer informatie over communicatiegedrag'.[67] Hij pleit daarom voor een heroverweging van de manier waarop dit type verkeersgegevens juridisch worden beschermd. Volgens hem kunnen IP-nummers (die het webdomein aangeven, bijvoorbeeld rijksoverheid.nl) als louter contactinformatie worden beschouwd en daarom als 'klassieke' verkeersgegevens worden behandeld, maar alle andere onderdelen van surfgegevens zouden meer juridische bescherming moeten krijgen dan klassieke verkeersgegevens (waarbij hij overigens in het midden laat of dat hetzelfde beschermingsniveau als communicatie-inhoud moet zijn).[68]

Volgens Koops hebben surfgegevens aanvullende bescherming nodig, niet zozeer omdat ze de interessesfeer blootgeven maar omdat 'een internetadres vaak direct [wijst] op de inhoud die wordt overgedragen.'[69] Ook Fischer vindt om deze reden dat surfgegevens extra bescherming nodig hebben; het zijn immers verkeersgegevens

> 'that link particular information contents to requesting individual users, while simultaneously revealing the nature of that content. In terms of sensitivity this is an important difference with regular traffic data, which in general do not disclose the content of the communication.'[70]

De (strafvorderlijke) wetgeving behandelt surfgegevens momenteel echter niet als inhoud, maar als verkeersgegeven:

> 'Ook de aanduiding van een website of een pagina binnen een website kan vallen onder het begrip verkeersgegevens. Een website en de pagina's binnen een website beschikken over een eigen nummer. Deze gegevens **geven inzicht in de belangstellingssfeer** van de gebruiker van telecommunicatie. Meer in het algemeen kan worden gesteld dat verkeersgegevens informatie kunnen opleveren over de soort instanties die benaderd worden door de gebruiker van telecommunicatie. Dit geeft informatie over de belangstellingssfeer van de gebruiker, net zoals zijn contacten met personen en instanties informatie over hem geven. Het **betreft echter niet het kennis nemen van (de inhoud van) de vertrouwelijke communicatie** van de gebruiker.'[71]

Men zou deze redenering kunnen lezen als een formalistische interpretatie van het begrip inhoud van communicatie, in de zin dat een Internetadres niet de boodschap is maar een adresgegeven waar de boodschap vandaan gehaald moet worden; dat is formalistisch, omdat het in principe een peulenschil is om met het adresgegeven de inhoud van wat er gecommuniceerd is (de inhoud van de opgevraagde webpagina) te achterhalen, zoals de Artikel 29 Werkgroep aangeeft. (Waarbij overigens aangetekend moet worden dat in het huidige Internetlandschap een Internetpagina veelal samengesteld wordt uit allerlei onderdelen, die lang niet altijd zijn te construeren aan de hand van een URL.) Een wellicht meer plausibele lezing (aangezien inhoud tussen haakjes staat) is dat de (strafproces)wetgever hier de nadruk legt op het feit dat Internetpagina's publiek zijn en dus niet vertrouwelijk zijn; de inhoud van opgevraagde

[64] 'Processing of header information (which might also include data on the content of the packets) should be considered as traffic data in the sense of Article 6 of Directive 97/66/EC (…)The list of websites visited by an Internet user (surfing behaviour) must in all cases be considered as traffic data (and *possibly* be given the same protection as content). Above all, this list should in principle be erased upon termination of the Internet session' (cursivering toegevoegd). Ibid., p. 51.
[65] MacGillavry 2004, p. 231.
[66] Smits 2006, p. 419.
[67] Ibid.
[68] Ibid., p. 399-400.
[69] Koops 2003, p. 68-69. In gelijke zin Steenbruggen 2009, p. 56.
[70] Fischer 2010, p. 35.
[71] *Kamerstukken II* 2001/02, 28 059, nr. 3, p. 7.

Internetpagina's is dus geen vertrouwelijke communicatie en zou om die reden niet onder het communicatiegeheim vallen. Om die reden vindt Patijn ook dat surfgegevens een sui-generiscategorie vormen:

> 'Verder omvat de informatie omtrent de bezochte pagina tevens informatie over de inhoud van de communicatie die heeft plaatsgevonden. (…) Ik bepleit de daarop betrekking hebbende verkeersgegevens aan te merken als een categorie sui generis. Gegevens over surfgedrag missen het neutrale karakter van verkeersgegevens bij de klassieke telefonie. Aan de andere kant betreft de uit de verkeersgegeven kenbare inhoud van de communicatie geen vertrouwelijke communicatie. De inhoud van een website is immers openbaar.'[72]

Vanwege het niet-neutrale karakter zouden verkeersgegevens niet als 'klassieke' verkeersgegevens moeten worden behandeld, maar vanwege het openbare karakter van webpagina's zouden ze ook niet als inhoud van (vertrouwelijke) communicatie moeten worden behandeld; vandaar Patijns pleidooi voor een sui generis-benadering. In de visie van de opstellers van het wetsontwerp-2012 is het echter niet relevant of de gegevens die via Internet worden verzonden publiek of privaat van aard zijn; het gaat om de gerichtheid van de communicatievorm, niet om het karakter van de inhoud. In de termen van het verkeersstromenmodel valt onder het correspondentiegeheim niet alleen de communicatie van een individu met een individueel informatiebestand (conversatie), maar ook communicatie van een individu met een centraal informatiebestand (consultatie).[73] Ook 'het opvragen van informatie bij een geautomatiseerde beldienst of internetdienst [wordt] vanwege [de] gerichtheid beschermd door artikel 13.'[74] Dat consultatie beschermwaardig is, blijkt ook uit het feit dat *video-on-demand* onder de reikwijdte van artikel 13 Gw valt.[75]

De kernvraag is dus niet of surfgegevens samenhangen met de inhoud van *vertrouwelijke* communicatie, maar of surfgegevens *dusdanig nauw* samenhangen met de inhoud van (niet-vertrouwelijke maar wel beschermde) communicatie dat zij als inhoud bescherming verdienen. Vaak is er een direct verband tussen een Internetadres en de inhoud die wordt overgedragen; door het Internetadres in te tikken ziet men immers de inhoud van de webpagina. Hoewel webpagina's in toenemende mate dynamisch worden, zijn er nog steeds veel (relatief) statische webpagina's (dat wil zeggen, waarvan de inhoud over langere tijd niet of weinig verandert), terwijl ook dynamische webpagina's vaak wel een deel inhoud bevatten dat relatief stabiel is. Aldus is het vaak eenvoudig om uit de URL de inhoud af te leiden van communicatie die van een webpagina naar een gebruiker is verstuurd. Het ligt daarom voor de hand om surfgegevens als inhoud te behandelen.

3.1.2. Zoekmachinesurfgegevens

Een bijzondere subcategorie van surfgegevens zijn surfgegevens van zoekmachines. Daarin is namelijk veelal de zoekterm opgenomen. '[I]nternetadressen kunnen bij zoekopdrachten ook inhoud (de zoektermen) bevatten.'[76] Jan Smits geeft hiervan het voorbeeld:[77]

> https://www.google.nl/webhp?sourceid=chrome-instant&rlz=1C1SKPC_enNL341&ion=1&ie=UTF-8#hl=nl&tbo=d&rlz=1C1SKPC_enNL341&sclient=psy-ab&q=internetconsultatie%20artikel%2013%20grondwet&oq=&gs_l=&pbx=1&fp=39b63b13594cdc97&bpcl=39650382&ion=1&bav=on.2,or.r_gc.r_pw.r_qf.&biw=1280&bih=933

waarin de zoekterm 'internetconsultatie artikel 13 grondwet' (hier rood weergegeven) is opgenomen. Naast het feit dat dit een surfgegeven is dat een direct verband houdt met de inhoud die wordt gecommuniceerd (van Google naar Jan Smits), bevat het ook letterlijk de inhoud van de communicatie van Jan Smits aan Google. Omdat het letterlijk de inhoud van communicatie weergeeft, zou het als inhoud moeten worden behandeld.[78] (Daarbij kan wel worden aangetekend dat het verkeersgegeven niet de inhoud bevat van de communicatie waar het betrekking op heeft – dat is namelijk de Internetpagina met de zoekmachineresultaten – maar de inhoud van een eerdere communicatie, namelijk de zoekvraag die voorafging aan de

[72] Patijn 2004, p. 135.
[73] Zie over het verkeersstromenmodel par. 4.3 en Smits 2013, p. 18.
[74] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 15.
[75] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 16.
[76] Koops 2003, p. 68.
[77] Smits 2013, p. 31.
[78] Zo ook Smits 2006, p. 399.

communicatie waar het verkeersgegeven betrekking op heeft. Dat is een aandachtspunt wanneer de wetgever de reikwijdte van artikel 13 Gw precies moet omschrijven, maar het lijkt mij als zodanig geen afbreuk te doen aan de beschermwaardigheid onder artikel 13. Het verkeersgegeven bevat immers inhoud van communicatie.)

Overigens moet er wel een onderscheid worden gemaakt tussen de zoekterm (die inhoud is maar geen verkeersgegeven) en de URL waarin de zoekterm is opgenomen (die een verkeersgegeven is dat inhoud bevat). Dat onderscheid wordt niet altijd scherp gemaakt:

> 'De *URL* die de zoekopdracht bevat kan als verkeersgegeven worden gezien. Maar evengoed valt te verdedigen dat *de opdracht* aan de zoekmachine een "communicatie" is, en dus als inhoud geclassificeerd moet worden.'[79]

De tweede zin staat in principe los van de eerste zin, omdat het om verschillende objecten gaat; de auteur bedoelt echter – neem ik aan – dezelfde objecten aan te duiden. Ook het wetsontwerp is niet consistent door 'de in een internetzoekmachine ingevoerde zoekterm' te bespreken *als een verkeersgegeven*, dat bescherming als inhoud verdient omdat het geheel of ten dele mede betrekking heeft op de inhoud van de communicatie.[80] Bedoeld wordt hier de URL waarin de zoekterm is weergegeven.

Overigens onderscheidt de lagere wetgever bij mijn weten surfgegevens van zoekmachines niet als een aparte categorie. In de strafvordering worden zoekmachinesurfgegevens daarom behandeld als surfgegevens en daarmee (zie par. 3.1) als verkeersgegeven en niet als inhoud. Ze vallen in het Besluit vorderen gegevens telecommunicatie onder 'het nummer van de natuurlijke persoon of rechtspersoon met wie de gebruiker verbinding heeft (…) gehad'.[81] In tegenstelling tot wat het wetsontwerp-2012 stelt,[82] zijn naar huidig recht in de strafvordering dus wel verkeersgegevens aangewezen die betrekking hebben op inhoud, maar niet als inhoud worden behandeld. Wanneer zoekmachinesurfgegevens, zoals de kennelijke bedoeling is van het wetsontwerp-2012, wel als inhoud onder artikel 13 Gw behandeld moeten worden, zal (de interpretatie van) de lagere wetgeving in dit opzicht dus aangepast moeten worden.

Voor de praktijk hoeft dat niet onoverkomelijk te zijn; het is in beginsel technisch eenvoudig om, door een filter te gebruiken, in een lijst met bezochte Internetadressen zoekresultaten van de meest gebruikte zoekmachines uit te sluiten. Opmerking verdient daarbij echter dat ook gewone webpagina's middels een zoekfunctie laten zien waarop binnen de pagina is gezocht. Zo levert het zoeken op de webpagina van BZK op de zoekterm 'grondwet' de volgende URL op:

> http://www.rijksoverheid.nl/zoeken?zoeken-op=grondwet

Het zal daarom, wanneer zoekmachinesurfgegevens moeten worden behandeld als inhoud, niet voldoende zijn om URL's van (bekende) zoekmachines uit een lijst met verkeersgegevens te verwijderen. In plaats daarvan kan wel bijvoorbeeld de padnaam – het gedeelte van een URL dat volgt na het protocol (bijvoorbeeld http://) en domein (bijvoorbeeld google.nl/) – worden verwijderd, of het gedeelte dat volgt na een '?', omdat zoekvragen in een URL meestal na een vraagteken worden weergegeven.[83]

3.1.3. Surfgegevens met inloggen

Een URL is niet alleen opgebouwd uit een protocol (bijvoorbeeld http, https of ftp), een domeinnaam (bijvoorbeeld rijksoverheid.nl) en een padnaam (bijvoorbeeld /documenten-en-publicaties/rapporten/2010/11/11/rapport-staatscommissie-grondwet.html), maar kan ook een poortnummer (zie par. 3.7) bevatten. Daarnaast is het ook mogelijk om authenticatiegegevens mee te geven aan een URL, zodat automatisch ingelogd kan worden. De URL is namelijk opgebouwd als volgt:[84]

> http://user:pass@voorbeeld.com:poortnummer/padnaam?zoekvraag#fragment

---

[79] Hes 2003, p. 16 (cursivering toegevoegd).
[80] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 32.
[81] Art. 2 onder c Besluit vorderen gegevens telecommunicatie, *Stb.* 2004, 394.
[82] 'Als verkeersgegevens zijn krachtens de artikelen 126n, 126u en 126zh Sv (in het Besluit vorderen gegevens telecommunicatie) alleen **gegevens** aangewezen **die niet geheel of ten dele mede op de inhoud van de communicatie betrekking** hebben.' Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 32.
[83] Zie http://nl.wikipedia.org/wiki/Uniform_Resource_Locator (geraadpleegd 15 januari 2013).
[84] http://nl.wikipedia.org/wiki/Uniform_Resource_Locator (geraadpleegd 15 januari 2013).

Jan Smits geeft een voorbeeld van een URL waarin een inlognaam is meegegeven:[85]

> http://kroonf3@gmail.com:V6XE7F@www.tql.nl

Deze URL, die uit een logbestand afkomstig is, bevat het emailadres (kroonf3@gmail.com) en het (versleutelde) wachtwoord (V6XE7F)[86] van een gebruiker die op de webpagina www.tql.nl inlogt.

Het hangt er enigszins van af hoe de authenticatiegegevens in de URL terechtkomen of het inhoud van een concrete communicatiehandeling (namelijk het versturen van inlognaam en wachtwoord) betreft, of dat het een automatisch geïntegreerd proces van een webpaginabezoek + inloggen betreft. In het eerste geval zijn de authenticatiegegevens vergelijkbaar met zoekmachinesurfgegevens: ze bevatten rechtstreeks inhoud van een (direct voorafgaande) communicatie. In het laatste geval zijn de authenticatiegegevens niet letterlijk inhoud van communicatie, maar ze betreffen wel duidelijk gegevens die onder verantwoordelijkheid van de verzender en niet onder die van de transporteur vallen. Het lijkt me ook evident dat dit type gegevens onder de ratio van het correspondentiegeheim bescherming als inhoud van communicatie verdient.

3.1.4. Conclusie

Bij surfgegevens in het algemeen is er vaak een direct verband tussen een Internetadres (URL) en de inhoud die wordt overgedragen; door het Internetadres in te tikken ziet men immers de inhoud van de webpagina. Surfgegevens zouden om die reden als inhoud moeten worden behandeld. Daarnaast geldt dat er specifieke onderdelen van surfgegevens zijn die wel rechtstreeks inhoud van communicatie afbeelden: in een URL die hoort bij een zoekopdracht staat veelal ook de zoekterm opgenomen, terwijl het ook mogelijk is dat een URL authenticatiegegevens bevat waarmee iemand inlogt op een webpagina. Hoewel het technisch mogelijk is om deze laatste typen gegevens uit te filteren uit een overzicht van bezochte webpagina's, versterkt het voorkomen van inhoud in URL's wel de algemene conclusie dat surfgegevens vaak direct verbonden kunnen worden met de inhoud van communicatie. Het ligt daarom meer voor de hand om alle surfgegevens integraal als inhoud te behandelen, dan om technische filters te gebruiken die bepaalde inhoudelijke onderdelen uit URL's filteren.

3.2. Email-onderwerpsveld

Het onderwerpsveld in een emailbericht is een van de duidelijkste voorbeelden van het grijze gebied tussen verkeersgegevens en inhoud:

> 'Hoe je die informatie [zoals de 'subject line' van een email], die in technische zin tot de verkeersgegevens behoort, maar die in feite veel over de inhoud vertelt, dient te behandelen, is in toenemende mate onduidelijk.'[87]

> 'Enerzijds lijkt het, naar de vorm, een verkeersgegeven, aangezien het over het netbericht gaat; anderzijds duidt het ook de inhoud aan, en wel zodanig dat het zelf als inhoud zou kunnen worden beschouwd. Veel netberichten hebben immers onderwerpen als "afspraak 20/8?" of "Norton SystemWorks 2002 Professional - 70% OFF - $29.99 with FREE UPS Ground Shipping! OptInFreebies Mailing List Member". (…) Het onderwerpsveld moet (…) beschouwd worden als inhoud'.[88]

> 'Voor wat betreft de onderwerpsregel in een mailbericht geldt dat het hier onmiskenbaar om gegevens met communicatieve elementen gaat. In sommige gevallen zal een onderwerpsregel zelfs het eigenlijke communicatiebericht inhouden.'[89]

Een voorbeeld van dat laatste is een (verder leeg) emailbericht waarvan de onderwerpsregel luidt: 'Goed interview op radio 1 ! Groeten, Ruud'.

---

[85] Smits 2013, p. 32. Letterlijk luidt de URL http://kroonf3%40gmail%2Ecom:V6XE7F@www.tql.nl/, ik heb voor het leesgemak hierin de hex codes die binnen URL's worden gebruikt (zie http://www.obkb.com/dcljr/charstxt.html (geraadpleegd 15 januari 2013)) vervangen door hun karakter (%40 is een apenstaart, %2E is een punt).
[86] Dit is het wachtwoord in versleutelde vorm, maar het kan wel worden gebruikt om in te loggen op de webpagina.
[87] Asscher en Ekker 2003, p. 104.
[88] Koops 2003, p. 77-78.
[89] Smits 2006, p. 420.

Het wetsontwerp-2012 schaart de onderwerpsregel dan ook zonder meer onder de inhoud van communicatie:

> 'Zo wordt het onderwerp van een e-mail in technische zin wel tot de verkeersgegevens betreffende die e-mail gerekend. Maar in juridische zin valt het onderwerp van een e-mail onder de reikwijdte van artikel 13 omdat dat onderwerp betrekking heeft op de inhoud van de e-mail.'[90]

Het kwalificeren van de onderwerpsregel als inhoud ligt ook voor de hand vanuit de in hoofdstuk 2 gegeven omschrijving van inhoud als datgene wat onder de verantwoordelijkheid van de afzender valt. De onderwerpsregel wordt vrijelijk gekozen door de verzender en de transporteur is er niet (als transporteur) aansprakelijk voor.

3.3. Sms-bericht

Een ander voorbeeld van een verkeersgegeven dat direct inhoud betreft, is een sms-bericht. Hiervoor geldt dan ook hetzelfde als voor de onderwerpsregel van een emailbericht:

> 'technisch gezien is een dergelijk bericht in zijn geheel een verkeersgegeven, maar juridisch gezien omvat een sms-bericht – naast verkeersgegevens – tevens de inhoud van communicatie.'[91]

Het is evident dat een sms-bericht onverkort als inhoud moet worden behandeld, aangezien de keuze voor de tekst van het sms-bericht geheel bij de verzender ligt.

3.4. Telefoon-keuzemenu's

Een minder vaak aangehaald voorbeeld van een grijs gebied betreft gegevens die worden gegenereerd in telefoon-keuzemenu's:

> 'Bij sommige geautomatiseerde telefoongesprekken geven verkeersgegevens veel inhoud weer ("wilt u informatie over seksueel overdraagbare aandoeningen, toets 1, wilt u een medische controle aanvragen, toets 2, wilt u een inenting, toets 3").'[92]

> '*Wij kunnen U sneller van dienst zijn indien U nu Uw BurgerServiceNummer intoetst:*
> De beller toetst: *123456789*
> Elk cijfer kent een andere toon; die tonen en daarmee de cijfers worden door de opgeroepene herkend en opgeslagen en vervolgens als sleutel gebruikt voor een zoekvraag in een database. Het systeem antwoordt terug:
> *Goedemiddag Meneer Smits waarmee kan de fiscus U van dienst zijn.*
> *1) Aanvragen van een VAR DGA*
> *2) Aanvragen van VAR WUO*
> *3) Aanvragen van een VAR*
> *Wanneer U geen keuze maakt wordt U zo spoedig mogelijk door een medewerker te woord gestaan*.'[93]

In technische zin gaat het hier om een grijs gebied tussen verkeersgegevens en inhoud. Het indrukken van toetsen ten behoeve van keuzemenu's betreft tweetonige signalen dan wel, bij moderne mobiele telefoons een aparte functie, die worden verzonden nadat de verbinding tot stand is gekomen. Ze worden daarom normaliter niet als zodanig gegenereerd of geregistreerd door de transporteur, maar alleen door de verzender en ontvanger. Tegelijkertijd zijn de ingetoetste nummers wel zichtbaar in het leesvenster van het ontvangende toestel, en in die zin betreft het wel in technische zin verkeersgegevens.[94]

Vanuit de functionele benadering van inhoud gaat het duidelijk om inhoud, aangezien de afzender en niet de transporteur bepaalt of er een 2 of een 8 wordt ingetoetst. Ook is de transporteur niet verantwoordelijk voor de inhoud van het keuzemenu, dat is namelijk de gesprekspartner van de beller. In die zin lijken de keuzetonen op een URL: het is een vorm van consultatie waarbij de centrale dienst gegevens aanbiedt en de beller een keuze maakt tussen deze gegevens. De gegenereerde gegevens (beltonen) vormen daarbij evenals de URL veelal een directe indicatie van de inhoud die wordt overgedragen (mijn BSN is 123456789; ik wil

[90] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 18.
[91] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 18.
[92] Koops 2003, p. 68n.
[93] Smits 2013, p. 25 (cursief in origineel).
[94] Ibid., p. 25-26.

informatie over seksueel overdraagbare aandoeningen). Dat is overigens alleen zo als de beltonen in verband (kunnen) worden gebracht met het keuzemenu (anders is een getallenreeks betekenisloos), maar dat zal in beginsel vaak het geval zijn omdat de overheid of een andere derde het telefoonnummer kan bellen en zelf het keuzemenu kan uitluisteren.

3.5. Emailadres

In de literatuur wordt ook een enkele keer gewezen op de mogelijkheid dat een emailadres inhoud kan bevatten. Bij webmail kunnen immers zelf adressen worden aangemaakt, zoals jaikkomnaarpetersfeestje@yahoo.com,[95] die een indicatie bevatten van de inhoud van berichten die naar dat adres worden toegestuurd. Ook is het tegenwoordig gebruikelijk bij Internettoegangsabonnementen dat gebruikers zelf vijf of tien emailadressen kunnen aanmaken, waarbij ze bijvoorbeeld adressen kunnen genereren als janjansen@aanbieder.nl, janjansen-zakelijk@aanbieder.nl, blondejan@aanbieder.nl, janwilseks@aanbieder.nl en postzegelverzamelaar@aanbieder.nl. Op zich hebben deze adressen niet als zodanig betrekking op communicatie, maar ze kunnen wel samenhangen met de communicatie die via die adressen verloopt. Zo zal het adres janwilseks@aanbieder.nl vermoedelijk alleen voor communicatie over seksafspraakjes worden gebruikt, terwijl een bericht van of aan postzegelverzamelaar@aanbieder.nl allicht over postzegels zal gaan. De samenhang met de inhoud van concrete berichten is hier echter veel minder nauw dan bij de onderwerpsregel van email en het adres geeft hooguit een zeer globale aanduiding van de vermoedelijke inhoud van communicatie. Alleen webmailadressen die voor een specifiek doel zijn aangemaakt, zoals jaikkomnaarpetersfeestje@yahoo.com, hangen tamelijk nauw samen met de (globale) inhoud van communicatie. Of een bericht een aanmelding of afmelding bevat (of spam) valt echter niet uit het emailadres af te leiden – tenzij bekend is dat er een parallel adres neeikkomhelaasnietnaarpetersfeestje@yahoo.com is aangemaakt.

Als zodanig is er dan ook geen directe reden om emailadressen als inhoud te behandelen. Echter, vanuit de functionele omschrijving van inhoud als datgene waarvoor de afzender en niet de transporteur verantwoordelijk is, zouden veel emailadressen tegenwoordig wel aangemerkt kunnen worden als inhoud. De keuze voor het adres (voor de apenstaart) ligt immers bij de gebruiker, niet bij de transporteur. En de keuze voor een bepaald emailadres heeft niet zelden een communicatieve functie, namelijk het profileren van de identiteit van de gebruiker – zoals bij blondejan@aanbieder.nl of kattenliefhebber@aanbieder.nl het geval is. In het kader van de vrijheid om vertrouwelijk te kunnen communiceren zou in het digitale tijdperk ook het communicatieve aspect van identiteitsconstructie via de keuze van een emailadres beschermd kunnen worden.

Dat staat overigens wel ver af van hoe tot nu toe in de literatuur en in de wetsgeschiedenis aangekeken wordt tegen het correspondentiegeheim. Men kan er ook voor kiezen deze vorm van identiteitsconstructie te beschermen via het algemene privacy- en dataprotectierecht,[96] waarbij in aanmerking moet worden genomen dat zelfgekozen emailadressen ook gevoelige persoonsgegevens kunnen bevatten, zoals ijsbrandgroenlinks@aanbieder.nl, dovejanjansen@aanbieder.nl of leerfetisjist@aanbieder.nl. Gezien de inhoudelijke component die emailadressen tegenwoordig hebben, moet de wetgever zich in elk geval afvragen of emailadressen nog simpelweg als (inhoudsloze) identificerende gegevens mogen worden beschouwd die door elke opsporingsambtenaar mogen worden gevorderd zonder bevel van een officier van justitie (art. 126na/ua/zi Sv).

3.6. Informatienummers en naambellen

Informatienummers *(premium rate numbers)* zijn telefoonnummers die voor bepaalde diensten worden gebruikt en veelal een andere prijsstructuur hebben, zoals 0800- en 0900-nummers.[97] Vroeger had men de nummers 002 en 003 om respectievelijk de tijd en het weerbericht op te vragen. Bij deze laatste nummers kan men uit de verkeersgegevens – nummer + tijd – vrijwel

[95] Koops 2003, p. 68n . Dit voorbeeld werd ontleend aan de werkelijkheid: het emailadres behoorde bij de verdediging van de dissertatie Blok 2002.
[96] Vgl. Agre 1998, Hildebrandt 2008.
[97] Zie http://nl.wikipedia.org/wiki/Informatienummer (geraadpleegd 15 januari 2013).

exact de inhoud afleiden. Bij 0800- en 0900-nummers is dat niet zo, behalve als bekend is dat een bepaald nummer geautomatiseerde berichten geeft volgens een vast patroon.

Daarnaast zijn er 0906-nummers voor erotische diensten en 0909-nummers voor amusement, spelletjes en prijsvragen. Uit de contactgegevens kan niet de precieze inhoud worden afgeleid, maar het nummer geeft wel een globale indicatie van de inhoud. Dat geldt ook voor sommige niet-geografische nummers, zoals 112 (alarmnummer) en 144 (meldpunt dierenmishandeling).

Ook bij het zogeheten naambellen[98] kan op basis van het gebelde nummer worden vermoed waar het gesprek globaal over gaat. Wie 0900-PIZZA belt, zal vermoedelijk een pizza bestellen, en wie 0900-NOTARIS belt, wil vermoedelijk iets juridisch regelen. Er kan echter niet worden afgeleid om welke pizza's of rechtshandelingen het gaat.

Informatienummers en naambellen zijn vergelijkbaar met zelfgekozen emailadressen (zie par. 3.5): ze hebben tot op zekere hoogte betrekking op de inhoud van communicatie en ze vallen – door de keuze voor een specifiek nummer of nummertype – onder verantwoordelijkheid van de gesprekspartner en niet van de transporteur. Ze betreffen echter niet de inhoud zelf en meestal (behoudens bij geheel geautomatiseerde nummers als 003) kan ook niet meer dan de globale context van de inhoud worden afgeleid uit het nummer. Systematisch valt er iets voor te zeggen om ze als inhoud te behandelen omdat de keuze van de betekenisvolle gegevens niet bij de transporteur maar bij de gesprekspartners ligt, maar evenals bij emailadressen staat dat ver af van hoe tot nu toe in de literatuur en in de wetsgeschiedenis aangekeken wordt tegen het correspondentiegeheim.

3.7. Poortnummers

Applicaties op Internet maken gebruik van verschillende poortnummers, zodat pakketjes op de juiste plaats op de bestemmingscomputer worden afgeleverd voor gebruik door de desbetreffende applicatie. Er zijn vele duizenden poortnummers, waarvan zo'n 1200 specifiek zijn toegewezen.[99] Zo wordt poort 104, evenals poorten 2761, 2762, 11112 gebruikt voor het Dicom-protocol (Digital Imaging and Communications in Medicine), waarmee informatie wordt uitgewisseld met of over medische afbeeldingen.[100] Poorten 3305 en 6619 worden gebruikt voor OFTP (Odette File Transfer Protocol), een protocol voor EDI (gestandaardiseerde uitwisseling van bedrijfsinformatie), poort 9212 voor het Financial Information eXchange-protocol, en poort 43594 voor het online multispelerspel RuneScape.[101]

Voor poortnummers geldt hetzelfde als voor informatienummers: ze geven een globale indicatie van de context waarin de communicatie plaatsvindt. Anders dan bij informatienummers ligt de keuze voor de koppeling van een bepaald poortnummer aan een bepaalde applicatie niet bij de communicatiepartners, maar bij de transporteur (in ruime zin: Internet-standaardiseringsorganisaties). Het zijn dus verkeersgegevens, maar ze geven wel een indicatie van het globale onderwerp van communicatie, bijvoorbeeld dat een medische scan wordt verstuurd of dat een gebruiker het spel RuneScape (en niet het spel Club Penguin Disney, waarmee poortnummer 6113 verbonden is) speelt.

3.8. Presentmelding

Bij diverse applicaties voor het onderhouden van contacten, wordt bij aanmelden en afmelden een bericht verzonden aan de contactpersonen (waarvoor de gebruiker toestemming heeft te geven om zijn aan- of afmelding te melden). Voorbeelden zijn MSN, Skype en WhatApp.[102] De melding van het apparaat van de gebruiker aan de apparaten van de contactpersonen wordt automatisch gegenereerd, maar dit gebeurt door de programmatuur van de eindgebruiker en niet door programmatuur van de transporteur. Het bericht met de strekking 'Jan Jansen is online' is dus communicatie die wordt beschermd onder het communicatiegeheim. Aan de verkeersgegevens van het bericht valt mogelijk de inhoud af te leiden, als het identificeerbaar is vanuit welke applicatie een bericht is verstuurd. In combinatie met tijdstip, zeker als de

[98] Zie onder http://nl.wikipedia.org/wiki/Naambellen#Gebruik_van_letters (geraadpleegd 15 januari 2013).
[99] http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers (geraadpleegd 15 januari 2013).
[100] http://en.wikipedia.org/wiki/Dicom (geraadpleegd 15 januari 2013).
[101] Zie http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers (geraadpleegd 15 januari 2013) en Smits 2013, p. 32-33.
[102] Zie ibid., p. 36.

verkeersgegevens over een bepaalde periode bekend zijn waardoor communicatiepatronen zichtbaar worden, zal dan duidelijk zijn dat de verzender de boodschap 'ik ben online en sta open voor communicatie' dan wel 'ik meld me af' heeft verstuurd.

3.9. Internet der dingen

In het Internet der dingen[103] (dat nog in ontwikkeling is maar wel dichterbij komt) hebben allerlei objecten een identificerende chip, voorzien van een IPv6-adres, die draadloos in verbinding staat met het Internet.[104] Zo kan de koelkast doorgeven aan de supermarkt dat er melk geleverd moet worden, of een vuilnisbak op straat aan de vuilnisdienst dat hij bijna vol zit. Sensoren in de kleding kunnen lichaamsfuncties monitoren en automatisch doorgeven, bijvoorbeeld aan een webdienst die statistieken over iemands hardlopen en gezondheid bijhoudt, of aan een alarmnummer als de hartslag en bloeddruk boven kritische drempels uitgaan. Wanneer bekend is dat een IP-adres behoort bij een koelkast, vuilnisbak of trainingspak, zal men globaal het onderwerp van de communicatie kunnen afleiden uit de verkeersgegevens. Het zal onbekend zijn wat een trainingspak precies doorgeeft aan de aanbieder van een gezondheids-app, maar het zal in elk geval meetresultaten van lichaamsfunctioneren betreffen. Vanwege de specificiteit van objecten in het Internet der dingen zal het verband tussen verkeersgegevens en inhoud vaak nauwer zijn dan bij communicatie via naambellen of poortnummers het geval is. Het betreft evenwel niet de letterlijke inhoud, maar hooguit het onderwerp en eventueel de strekking van communicatie.

3.10. Locatiegegevens

Een aanbieder van mobiele telefonie moet weten waar een mobiele telefoon zich bevindt, om een gesprek of bericht door te kunnen geleiden. Daarom worden in het netwerk – als de telefoon aan staat – doorlopend locatiegegevens gegenereerd: de telefoon meldt zich bij de dichtstbijzijnde zendmast, die de locatie van de telefoon doorgeeft aan dienstaanbieder. Wanneer iemand met een mobiele telefoon daadwerkelijk communiceert, wordt ook het gegeven meegestuurd via welke zendmast de communicatie verloopt. Deze gegevens vallen onder de verantwoordelijkheid van de telecomaanbieder en zijn, volgens het Europese telecommunicatierecht, dus verkeersgegevens:

> 'In digitale mobiele netwerken worden locatiegegevens betreffende de geografische positie van de eindapparatuur van de mobiele gebruiker verwerkt om de transmissie van de communicatie mogelijk te maken. Dergelijke gegevens zijn verkeersgegevens'.[105]

Locatiegegevens worden vaak genoemd in literatuur over de privacy van telecommunicatie. Deels gaat dat over de vraag of locatiegegevens die worden gegenereerd wanneer een toestel in de paraatstand staat, wel of niet verkeersgegevens zijn; ze hangen immers niet samen met een concrete belhandeling en vallen daarom niet altijd onder de juridische definities van verkeersgegeven.[106] De vraag of locatiegegevens, voor zover ze verkeersgegevens zijn (dus wanneer ze samenhangen met een concrete communicatiehandeling), ook inhoud kunnen betreffen, komt echter niet aan de orde in de literatuur.

Auteurs bespreken meer in het algemeen de privacygevoeligheid van locatiegegevens. Arno Smits merkt op dat een mobiele telefoon als peilbaken kan gaan fungeren, zeker als de mobiele telefoon veel wordt gebruikt.[107] Vanwege de grotere privacygevoeligheid zouden locatiegegevens van mobiele telefoons volgens hem dan ook alleen met rechterlijke machtiging moeten kunnen worden opgevraagd.[108] Koops wijst op 'verfijnde' locatiegegevens die samenhangen met toegevoegdewaardediensten (zoals bedoeld in art. 9 Richtlijn 2002/58/EG), dat wil zeggen precieze locatiegegevens op basis van bijvoorbeeld driehoeksmeting.

> 'Zeker bij toegevoegdewaardediensten kan dit meer informatie opleveren, bijvoorbeeld wanneer iemand automatisch aanbiedingen op zijn mobiele toestel ge-sms't krijgt van de restaurants of

[103] Zie http://en.wikipedia.org/wiki/Internet_of_things (geraadpleegd 15 januari 2013).
[104] Zie Smits 2013, p. 33-34.
[105] Richtlijn 2002/58/EG, overweging 35.
[106] Zie Hes 2003, p. 37; Ekker 2003, p. 46; Asscher en Ekker 2003, p. 106; Smits 2006, p. 386.
[107] Smits 2006, p. 369-370.
[108] Ibid., p. 386.

supermarkten waar hij langs rijdt. Justitie kan dan op basis van de verkeersgegevens bijvoorbeeld een nauwkeurige route bepalen waar iemand heeft gereden.'[109]

Volgens Fischer kunnen verkeersgegevens daarom soms privacygevoeliger zijn dan de inhoud van communicatie:

'It is possible for traffic data to surpass the sensitivity of the communication content. Such can be the case with location data, a form of traffic data in mobile telephony. The telephone conversation (communication content) may be insignificant, but the relating location data may reveal a person's whereabouts, which are sometimes significant.'[110]

De literatuur geeft aldus blijk van een bezorgdheid over de bescherming van locatiegegevens, vanwege het inzicht dat deze kunnen bieden in de verblijfplaatsen en bewegingspatronen van personen. Het belang van bescherming daarvan heeft echter niet primair te maken met de vrijheid om onbevangen privé te kunnen communiceren, maar meer met het algemene belang van privacy in het licht van de bewegingsvrijheid. Niettemin bestaat er wel een correlatie met het correspondentiegeheim. Vanuit de ratio die Asscher formuleerde – 'het vertrouwen dat de burger stelt in het communicatiekanaal kan worden aangetast, wanneer verkeersgegevens worden verwerkt voor doelen die niet noodzakelijkerwijs voortvloeien uit het leveren van deze dienst'[111] – kan het verwerken van locatiegegevens voor andere doeleinden een verkillend effect hebben op de vrijheid van burgers te communiceren. Iemand zou zich bijvoorbeeld geremd kunnen voelen om te bellen wanneer hij zich in het gebied van de Amsterdamse Wallen bevindt, of wanneer een werknemer met een mobiele telefoon van het bedrijf een polikliniek bezoekt voor een medische klacht die hij (vooralsnog) voor de baas verborgen wil houden.

Het feit dat locatiegegevens beschermwaardig zijn vanuit de ratio van het correspondentiegeheim, staat echter los van de vraag of zij (alleen) verkeersgegevens zijn of (ook) inhoud. Hoewel de literatuur locatiegegevens niet koppelt aan de inhoud van communicatie, zal er in sommige gevallen wel een bepaald verband bestaan tussen een locatiegegeven en de (vermoedelijke) inhoud van een bericht. In het voorbeeld van de toegevoegdewaardediensten, zal het voor de hand liggen dat een sms van Albert Heijn aan een gebruiker die wordt verstuurd op een plaats en tijd dat de gebruiker zich binnen een straal van 500 meter van een Albert Heijn bevindt, een boodschap bevat over die Albert Heijn-vestiging en met een paar aanbiedingen van de week. Ook de inhoud van een sms-bericht van restaurant De Lange Muur aan een gebruiker van een toegevoegdewaardedienst die om 18:05 op de hoek van de straat van het restaurant rijdt, laat zich globaal raden. Met hoge waarschijnlijkheid weet men waarover een sms gaat die verzonden is in de nabijheid van De Grolsch Veste 30 seconden nadat Castaignos gescoord heeft. In het algemeen zal het echter minder waarschijnlijk zijn dat globaal uit tijd en plaats is af te leiden waarover een bepaalde communicatie ging. Duidelijk is echter wel dat in diverse gevallen – zeker als er verkeersgegevens over een langere periode beschikbaar zijn waaruit patronen zijn af te leiden – er een zekere correlatie kan bestaan tussen locatiegegevens (in combinatie met tijdstip) en de vermoedelijke globale inhoud van een communicatie.

3.11. Data mining

Door middel van *data mining* kunnen grote databestanden worden doorzocht om verbanden te vinden. Dit levert nieuwe kennis op, die met de groei van de informatiesamenleving in toenemende mate een gedetailleerd beeld van het persoonlijk leven van individuen kan betreffen.[112] Toegepast op verkeersgegevens kan *data mining* ook veel kennis opleveren.

Steenbruggen betoogt daarom dat de vooronderstelling dat inhoud per definitie gevoeliger is dan verkeersgegevens, nuancering behoeft. Op grond van verkeersgegevens kunnen 'door derden uitermate gedetailleerde communicatie- en interesseprofielen van gebruikers worden opgesteld. Onder omstandigheden kan deze informatie veel gevoeliger zijn dan de uitgewisselde informatie zelf.'[113] Hofman geeft daar een voorbeeld van: uit een bepaald communicatiepatroon zou bijvoorbeeld afgeleid kunnen worden dat mevrouw Y een verhouding heeft met de chef.

[109] Koops 2003, p. 82.
[110] Fischer 2010, p. 5n .
[111] Asscher 2003, p. 24; zie noot 33 en bijbehorende tekst.
[112] Zie algemeen Hildebrandt en Gutwirth 2008.
[113] Steenbruggen 2009, p. 56-57.

‘Hieruit blijkt dat ook verkeersgegevens direct of indirect zeer gevoelig kunnen zijn met het oog op de persoonlijke levenssfeer.’[114]

Ekker geeft aan dat men door het koppelen van verkeersgegevens aan andere data men niet alleen veel te weten komen over het communicatiegedrag van personen en hun feitelijk handelen, maar soms ook over de inhoud van de communicatie.[115]

> ‘Soms kan zodoende worden vastgesteld wat (ongeveer) de inhoud van de communicatie is geweest:
>
> - Alice heeft gebeld met haar advocaat, haar psycholoog, het ziekenhuis, de nummerinformatie van de PTT, de Sociale Dienst, het Bureau Kredietregistratie, of het alarmnummer van de brandweer.
> - Alice heeft ingelogd op de website van Alcoholics Anonymous en deelgenomen aan een chatsessie.
> - Alice heeft ingelogd op de website van de gemeente Amsterdam en op een bulletin-board kritiek geuit op het parkeerbeleid van de gemeente.
> - Alice heeft van de website van een politieke partij het partijprogramma gedownload en een folder besteld waarmee zij lid kan worden van die partij.[116]
>
> (…) Daarnaast kunnen verkeersgegevens iets zeggen over de inhoud van communicatie wanneer men ze combineert met andere informatie. Hieruit volgt een belangrijke constatering: informatie over het communicatiegedrag van individuen en soms ook de inhoud van de communicatie kan worden verkregen door verkeers- en persoonsgegevens met elkaar te combineren.’[117]

Met andere woorden, diverse van de hierboven geschetste grijze gebieden, waarbij verkeersgegevens een globale indicatie kunnen geven van de inhoud, worden nog grijzer wanneer verkeersgegevens gecombineerd worden met andere databestanden. De combinatie van gegevens kan de interpretatie van wat bepaalde verkeersgegevens over de inhoud van een bepaalde communicatie vertellen, aanscherpen dan wel waarschijnlijker maken. Het koppelen van verkeersgegevens met andere politiegegevens in het kader van opsporing is niet onderworpen aan een rechterlijke machtiging (zie art. 11 WPolG). Van belang is daarbij dat de politie (evenals de veiligheidsdiensten) via openbrononderzoek door middel van geautomatiseerde systemen, zoals iColumbo, op een laagdrempelige manier (zonder rechterlijke machtiging) veel data kan verzamelen over personen.[118] De combinatie van data uit open bronnen en verkeersgegevens zou meer mogelijkheden kunnen bieden om verkeersgegevens in context te plaatsen en daarmee meer inzicht te krijgen in de vermoedelijke inhoud van een bericht dan bij analyse van losstaande verkeersgegevens mogelijk is.

3.12. Conclusie

In dit hoofdstuk zijn grijze gebieden behandeld die bestaan tussen verkeersgegevens en inhoud, waarmee de tweede deelvraag van dit onderzoek is beantwoord. De belangrijkste grijze gebieden die in de literatuur worden genoemd, zijn surfgegevens (waaronder ook zoekmachinesurf-gegevens) en de onderwerpregel in een emailbericht en een sms-bericht. Deze laatste twee zijn technisch verkeersgegevens, maar juridisch duidelijk te kwalificeren als inhoud, omdat ze deel uitmaken van de feitelijke inhoud die onder verantwoordelijkheid van de verzender valt. Om deze reden zijn ook toonkeuzes die bij telefoon-keuzemenu’s worden gebruikt, inhoud. Surfgegevens zijn niet letterlijk inhoud, maar wijzen vaak wel direct op de inhoud die tussen webpagina’s en webgebruikers wordt getransporteerd. Het publieke karakter van deze inhoud doet daarbij niet af aan de eventuele beschermwaardigheid onder het communicatiegeheim; de beschermwaardigheid hangt af van de vraag of een URL dusdanig nauw samenhangt met de inhoud dat deze op dezelfde manier als inhoud beschermd zou moeten worden. Bij zoekmachinesurfgegevens is dat verband in elk geval directer, omdat zoektermen – die inhoud

[114] Hofman 1995, p. 51.
[115] Ekker 2003, p. 47.
[116] Ibid., p. 48.
[117] Ibid.
[118] Zie Koops e.a. 2012a.

van communicatie zijn – vaak deel uitmaken van de URL van de pagina met zoekresultaten; hetzelfde geldt mutatis mutandis voor URL's die authenticatiegegevens voor inloggen bevatten.

Minder prominent worden in de literatuur soms andere grijze gebieden gesignaleerd. Het betreft dan emailadressen, informatienummers en naambellen, waarbij de zelfgekozen adressen een betekenis hebben die uitstijgt boven inhoudsloze adressen, waardoor enige samenhang ontstaat tussen het adres en de vermoedelijke globale inhoud van communicatie via dat adres. Dat geldt grosso modo ook voor poortnummers, de presentmelding bij webapplicaties en het Internet der dingen, waarbij er om uiteenlopende redenen enige correlatie bestaat tussen het gegeven dat communicatie plaatsvindt en de vermoedelijke globale inhoud van het berichtenverkeer. Het verband tussen verkeersgegevens en inhoud is in deze grijze gebieden minder sterk dan bij surfgegevens. Niettemin kan in bepaalde gevallen de context dusdanig zijn dat met behoorlijke waarschijnlijkheid het onderwerp, en soms ook de strekking, van communicatie kan worden afgeleid, zeker als verkeersgegevens over lange tijd beschikbaar zijn en/of gecombineerd worden met andere gegevens.

De opkomst van *data mining* versterkt de mogelijkheid dat verkeersgegevens onder omstandigheden inzicht bieden in de vermoedelijke inhoud van een bericht, maar kan ook leiden tot andersoortige inzichten in de persoonlijke levenssfeer van burgers. De literatuur weerspiegelt een bezorgdheid over de toenemende privacygevoeligheid van verkeersgegevens, die niet alleen communicatie- maar ook gedragspatronen kunnen blootleggen. Locatiegegevens zijn daarvan het prangendste voorbeeld. Soms zullen verkeersgegevens, ongeacht of ze verband houden met inhoud, dan ook gevoeliger zijn dan de inhoud van communicatie zelf. Naast de vraag die in dit onderzoek centraal staat, namelijk welke typen verkeersgegevens beschermwaardig zijn onder artikel 13 Gw gezien de ratio en functie van het correspondentiegeheim, is daarom een even belangrijke vraag voor de wetgever hoe verkeersgegevens afdoende juridisch beschermd kunnen worden gezien hun privacygevoeligheid in het algemeen.

4. Een typologie van verkeersgegevens

Nu de grijze gebieden in kaart zijn gebracht, is de vraag of deze op een zinvolle en werkbare manier kunnen worden geclusterd, zodat een classificatie ontstaat van verkeersgegevens aan de hand waarvan kan worden bepaald of verkeersgegevens al dan niet als inhoud zouden moeten worden behandeld. Hieronder worden verschillende mogelijke classificaties besproken, variërend van abstract-theoretisch tot meer concreet-pragmatisch.

4.1. Een conceptuele typologie

Een conceptuele typologie knoopt aan bij de conceptuele invulling van inhoud en verkeersgegevens. Deze begrippen kunnen, zoals betoogd in hoofdstuk 2, als volgt worden ingevuld:

- inhoud is datgene wat onder verantwoordelijkheid van de verzender valt;
- verkeersgegevens zijn gegevens die onder verantwoordelijkheid van de transporteur (als transporteur) vallen. Dit betreft, in de vorm van Fischer's 3x3-matrix, gegevens die nodig zijn voor
    - dienstuitvoering,
    - dienstafrekening of
    - dienstbeheer,

  door aanbieders van *mere conduit*, *caching* en *hosting*.[119]

De vraag of gegevens (primair) onder verantwoordelijkheid van de communicatiepartner(s) of onder die van de transporteur vallen, biedt een nuttig criterium om gegevens te classificeren. Het criterium werkt bijvoorbeeld goed om te onderbouwen waarom de email-onderwerpregel en het sms-bericht inhoud zijn en geen verkeersgegevens. Bij hybride gegevens, zoals de zoekmachine-URL die automatisch gegenereerd wordt ten behoeve van het transport maar die ook door de gebruiker gekozen inhoud bevat, geeft het criterium aan dat het gedeelte achter het "?" in de zoekmachine-URL (ook) inhoud is en wat daaraan voorafgaat (alleen) een verkeersgegeven. Bij andere grijze gebieden is het criterium echter niet eenduidig toepasbaar, omdat er daar een minder duidelijke correlatie bestaat tussen het verkeersgegeven en de inhoud van een concreet bericht. Er kan een hybride verantwoordelijkheid zijn, waarbij de transporteur grotendeels of geheel verantwoordelijk is voor een bepaald gegeven, en het dus strikt genomen niet om inhoud gaat, maar waarbij het verkeersgegeven wel in zekere mate correleert met de inhoud. Dat is bijvoorbeeld het geval bij poortnummers (zie par. 3.7) of bij emailadressen, die beheerd worden door de aanbieder maar waarbij de gebruiker een zekere mate van keuzevrijheid heeft voor de invulling ervan.

Daarom kan een nadere conceptuele indeling worden gezocht om te helpen gegevens te classificeren als inhoud of als verkeersgegeven. Omdat het gaat om de manieren waarop verkeersgegevens kunnen relateren aan inhoud, ligt het voor de hand hiervoor het onderscheid uit de semiotiek te hanteren in verschillende soorten tekenrelaties. C.S. Peirce, de grondlegger van de semiotiek, heeft een onderscheid gemaakt in de manier waarop een teken naar een object kan verwijzen. Een teken kan verwijzen naar het object in de vorm van een:[120]

1. ***icoon***: een teken dat lijkt op het object, vanwege een bepaalde eigenschap die zowel het teken als het object hebben; daarvan zijn er drie soorten:
    a. ***afbeelding***: het teken lijkt op het object door een simpele gedeelde eigenschap, zoals een foto lijkt op de afgebeelde persoon of een onomatopee ("woef") op een geluid;
    b. ***diagram***: het teken lijkt op het object doordat de interne relaties tussen onderdelen vergelijkbaar zijn, zoals een stroomschema van een elektrische schakeling, of een organogram van een organisatie;
    c. ***metafoor***: het teken lijkt op het object door een andersoortige parallel, die abstracter is dan de simpele gedeelde eigenschap van de afbeelding; zo lijkt een computervirus

[119] Zie noot 57 en bijbehorende tekst.
[120] De beschrijving is ontleend aan http://en.wikipedia.org/wiki/Semiotic_elements_and_classes_of_signs onder "Icon, index, symbol" (geraadpleegd 15 januari 2013).

niet letterlijk op een virus maar wel figuurlijk, door de eigenschappen onzichtbaar te zijn en zichzelf te vermenigvuldigen; daarom is 'virus' een metafoor voor bepaalde typen kwaadaardige programmatuur;

2. ***index***: een teken dat verwijst naar een object door een feitelijke relatie in de werkelijkheid, zoals een richtingaanwijzer met daarop 'Den Haag' naar Den Haag wijst, of een inhoudsopgave verwijst naar de inhoud van een document;
3. ***symbool***: een teken dat verwijst naar een object op basis van een gewoonte of afspraak, zoals de kleur rood verwijst naar gevaar, een verbod of karnemelk en de kleur groen naar milieuvriendelijkheid, een permissie of een giftige stof.

Deze typologie zou kunnen helpen om het verband tussen verkeersgegevens en inhoud nader te duiden. Zo is een sms een 1-op-1 afbeelding van de inhoud en is de onderwerpregel van een emailbericht een afbeelding van de inhoud omdat het meestal het onderwerp (en vaak de kern daarvan) omschrijft. Een URL verwijst indexicaal naar de inhoud van communicatie, omdat het direct verbonden is met de webpagina waarvan de inhoud wordt getransporteerd naar de gebruiker. Bij sommige opeenvolgingen van communicaties weerspiegelt de volgorde van typen berichten de vermoedelijke inhoud: als gebruiker A via een webformulier een bericht aan webpagina B stuurt, waarna direct een email van domein B naar A wordt gestuurd, en vervolgens A dertig seconden later een nieuwe URL van B aanklikt, is het zeer waarschijnlijk dat het ingevulde webformulier een aanmelding bevatte, het emailbericht van B naar A een verzoek om de aanmelding te bevestigen, en de laatste URL een bevestiging van aanmelding. Zo vormt de direct opeenvolgende sequentie van webformulier-email-URL een diagram van de communicatie van een aanmelding.

Bij de presentmelding is het feit dat een bericht van een gebruiker naar diens contacten wordt verstuurd, een metafoor voor de inhoud "ik ben er weer". Sommige voorbeelden van locatiegegevens staan symbool voor de inhoud, wanneer er een sterk statistisch verband bestaat tussen de verkeersgegevens (op tijdstip x op plaats y een sms verzonden) en de vermoedelijke inhoud van het bericht ("U gaat nu de grens over"; "Aanbieding van De Lange Muur"; "Castaignos scoort 2-0!").

In het algemeen hebben afbeeldingen en diagrammen een sterk verband met het object waarnaar zij verwijzen, bij de afbeelding vanwege de eigenschap waarin het object zichtbaar is, bij het diagram vanwege de gelijkenis in structuur. Ook bij de index is het verband tamelijk sterk vanwege de feitelijke nabijheidsrelatie. Metaforen en symbolen hebben vaak een zwakker verband: ze verwijzen weliswaar naar het object, maar geven daarbij minder intrinsiek informatie over het object. Daarbij moet wel worden opgemerkt dat dit niet altijd zo is: een afbeelding of diagram kan zwak zijn doordat het slechts een enkele eigenschap of een abstracte structuur van het object weerspiegelt, terwijl een krachtige metafoor of sterk symbool treffend de kern van een object kan aanduiden.

In gevallen waarin het criterium of gegevens onder verantwoordelijkheid van de communicatiepartner(s) vallen, niet voldoende houvast biedt, kan de vervolgvraag worden gesteld of het verband tussen het verkeersgegeven en inhoud de vorm heeft van een afbeelding of diagram, van een index, of van een metafoor of symbool. In het geval het verkeersgegeven een afbeelding of diagram is van de inhoud, valt het in beginsel te kwalificeren als inhoud (tenzij het om een zwakke afbeelding of een abstract diagram gaat). Als het de vorm heeft van een index, is het als inhoud te kwalificeren als de overheid de feitelijke koppeling kan volgen tussen verkeersgegeven en inhoud; dat is typisch het geval bij surfgegevens. Als het echter de vorm heeft van een metafoor of symbool, kan het als verkeersgegeven worden behandeld en niet als inhoud (tenzij het om een sterke metafoor of sterk symbool gaat dat de kern van de inhoud aanduidt). Op deze manier valt bijvoorbeeld een onderscheid te maken in zelfgekozen emailadressen die een inhoudelijke (dat wil zeggen identiteitsconstruerende) component hebben: de meeste daarvan staan symbool voor de (vermoedelijke) globale inhoud van een bericht, omdat gewoonlijk een bericht van postzegelverzamelaar@aanbieder.nl over postzegels zal gaan, en een bericht van janwilseks@aanbieder.nl gewoonlijk iets met seks te maken zal hebben. Omdat het om een zwakke tekenrelatie gaat, kunnen dit soort emailadressen als verkeersgegevens en niet als inhoud worden behandeld. Sommige emailadressen wijzen echter op de kern van de vermoedelijke communicatie, zoals jaikkomnaarpetersfeestje@yahoo.com, in welk geval het emailadres (vergelijkbaar met een emailonderwerpregel) een afbeelding wordt van de inhoud. Het zou in dat geval dan ook als inhoud moeten worden behandeld. (Dat roept wel de

vraag op of het praktisch mogelijk is een onderscheid te maken *binnen* een bepaalde categorie, zoals emailadressen. Op die vraag kom ik in hoofdstuk 6 terug.)

Samenvattend kan men de volgende conceptuele typologie van verkeersgegevens maken, ten behoeve van de afbakening tussen verkeersgegevens en inhoud:

classificeringsvraag	**inhoud?**	**voorbeelden**
1. Onder wiens verantwoordelijkheid valt het gegeven?		
a. communicatiepartner(s)	ja	sms-bericht emailonderwerpregel URL van zoekmachine na "?": zoeken-op=grondwet
b. transporteur, en het gegeven biedt geen inzicht in inhoud	nee	locatiegegeven mobiele telefoon URL van zoekmachine tot en met "?": http://www.rijksoverheid.nl/zoeken?
c. transporteur, en het gegeven biedt mogelijk zicht op de inhoud	bepalen aan hand van vraag 2	
2. Op welke manier verwijst het verkeersgegeven naar de inhoud?		
a1. afbeelding (regel)	ja	geautomatiseerd toetsmenu: "toets nu uw BSN in" berichtspecifiek emailadres:[121] jaikkomnaarpetersfeestje@yahoo.com berichtspecifiek informatienummer: 0906-BLOWJOB
a2. afbeelding (uitzondering: zwak verband)	nee	inhoudspecifiek emailadres:[122] petersfeestje@yahoo.com inhoudspecifiek informatienummer: 0900-NOTARIS
b1. diagram (regel)	ja	patroon van webaanmelding + emailbevestiging
b2. diagram (uitzondering: zwak verband)	nee	
c1. metafoor (regel)	nee	telefoonnummer 144 ("red een dier")
c2. metafoor (uitzondering: sterk verband)	ja	telefoonnummer 112 + locatie + tijdstip presentmelding bij Internetapplicaties
d1. index (regel)	ja	geautomatiseerd telefoonkeuzemenu: "voor inentingen, toets 3" URL met (min of meer) vaste inhoud: http://nl.wikipedia.org/wiki/Uniform_Resource_Locator URL met flexibele inhoud + tijdstip: http://www.nu.nl/ op maandag 12 januari om 13:52
d2. index (uitzondering: koppeling niet te maken)	nee	URL met flexibele inhoud zonder datum/tijd: http://www.nu.nl/
e1. symbool (regel)	nee	informatienummer: 144, 0906-1234 poortnummer voor financiële of medische applicatie emailadres met inhoudelijke component: postzegelverzamelaar@aanbieder.nl

[121] Met 'berichtspecifiek' bedoel ik dat het verkeersgegeven dusdanig concreet is dat het een indicatie geeft niet alleen van het vermoedelijke onderwerp maar ook van de vermoedelijke strekking van een bericht.

[122] Met 'inhoudspecifiek' bedoel ik dat het verkeersgegeven concreet genoeg is om het vermoedelijke onderwerp aan te duiden, maar niet concreet genoeg om de strekking van berichten uit af te leiden.

classificeringsvraag	inhoud?	voorbeelden
e2. symbool (uitzondering: sterk verband)	ja	contextspecifiek locatiegegeven (gekoppeld aan toegevoegdewaardedienst): sms van restaurant X aan mobiel Y in de buurt van X

Tabel 1. Een conceptuele typologie van verkeersgegevens

Een voordeel van deze typologie is dat het houvast biedt om op basis van inhoudelijke argumenten een verkeersgegeven al dan niet als inhoud te classificeren. Een nadeel is dat het ook een onderscheid maakt in verkeersgegevens als telefoonnummers en emailadressen, afhankelijk van de mate waarin die inzicht bieden in de inhoud van communicatie, terwijl de rechtspraktijk tot nu toe gegevens als nummers integraal behandelt als verkeersgegevens. De classificering van verkeersgegevens tot nu toe is dan ook meer functioneel dan conceptueel van aard.

4.2. Een functionele typologie

De rechtspraktijk kent verschillende opsommingen van typen verkeersgegevens. De twee belangrijkste zijn de aanwijzing van verkeersgegevens die kunnen worden gevorderd en de aanwijzing van verkeersgegevens die telecommunicatieaanbieders moeten bewaren.
Het Besluit vorderen gegevens telecommunicatie wijst de volgende typen gegevens aan als verkeersgegevens:

a. 'de naam, het adres en de woonplaats van de gebruiker;
b. de nummers van de gebruiker;
c. de naam, het adres, de woonplaats en het nummer van de natuurlijke persoon of rechtspersoon met wie de gebruiker verbinding heeft, heeft gehad of heeft getracht tot stand te brengen, of van de natuurlijke persoon of rechtspersoon die heeft getracht met de gebruiker verbinding tot stand te brengen;
d. de datum en het tijdstip waarop de verbinding met de gebruiker tot stand is gebracht en beëindigd en de duur van de verbinding, dan wel, ingeval er geen verbinding tot stand is gekomen, de datum en het tijdstip waarop is getracht verbinding met de gebruiker tot stand te brengen (…);
e. de locatiegegevens van het netwerkaansluitpunt dan wel gegevens betreffende de geografische positie van de randapparatuur van een gebruiker ingeval van een verbinding of poging daartoe;
f. de nummers van de randapparatuur waarvan de gebruiker gebruik maakt of heeft gemaakt;
g. de soorten diensten waarvan de gebruiker gebruik maakt of heeft gemaakt evenals de daarbij behorende gegevens;
h. de naam, het adres en de woonplaats van degene die de rekening betaalt voor de openbare telecommunicatiediensten en telecommunicatienetwerken die de gebruiker ter beschikking heeft of heeft gehad, indien deze een ander is dan de gebruiker.'[123]

Op basis van de Wet bewaarplicht telecommunicatiegegevens, moeten telecomaanbieders de diverse typen gegevens bewaren, die grotendeels neerkomen op naam- en adresgegevens, nummers, type dienst, datum/tijdgegevens, en (bij mobiele telefonie) locatiegegevens.[124]

Anton Ekker heeft een classificering van verkeersgegevens gemaakt die deze gegevens groepeert naar het object van het verkeersgegeven: communicatiegedrag algemeen, routering en vorm en omvang.[125] Deze classificering biedt een antwoord op de klassieke vragen: wie, wat, waar, wanneer en hoe? Ze kunnen daarom worden samengenomen in de volgende typologie:

object van het gegeven	type verkeersgegeven	vragen
communicatiegedrag algemeen	duur	wanneer
	tijdstip (begin, eind), datum	
	locatie eindapparatuur	waar
	type dienst	wat

[123] Art. 2 Besluit vorderen gegevens telecommunicatie, *Stb.* 2004, 394.
[124] Zie Bijlage behorende bij art. 13.2a Telecommunicatiewet, ingevoerd bij Wet bewaarplicht telecommunicatiegegevens, *Stb.* 2009, 333.
[125] Ekker 2003, p. 45.

routering	adres/nummer verzender adres/nummer ontvanger	wie
vorm en omvang	volume (omvang) gebruikte protocol formaat	wat hoe

Tabel 2. Typologie naar object van verkeersgegevens

De waarom-vraag komt hierin niet aan de orde. Deze hangt samen met een tweede classificering van Ekker, naar het doel van de verwerking: transmissie, facturering, of toegevoegdewaardedienst. Dit lijkt op de drie functies die Fischer onderscheidt, maar de derde categorie (toegevoegdewaardediensten bij Ekker, dienstbeheer bij Fischer) verschilt. Ekkers indeling is gebaseerd op Richtlijn 2002/58/EG, die een toegevoegdewaardedienst definieert als een 'dienst die de verwerking vereist van verkeersgegevens of locatiegegevens anders dan verkeersgegevens, en die verder gaat dan hetgeen nodig is voor het overbrengen van een communicatie of de facturering ervan'.[126]

Een typologie naar doel van verwerking is bruikbaarder dan bovenstaande typologie naar object van verkeersgegevens, als het gaat om het afbakenen van verkeersgegevens tegenover inhoud. Over het algemeen bieden verkeersgegevens die worden verwerkt ten behoeve van facturering of dienstbeheer namelijk geen zich op de inhoud. De voorbeelden in de grijze gebieden betreffen namelijk verkeersgegevens die worden verwerkt voor transmissie of voor een toegevoegdewaardedienst.[127] De gegevens uit het Besluit vorderen gegevens telecommunicatie kunnen aan de hand van deze doelen dan als volgt worden gegroepeerd:

doel van verwerking (aanbieder)	**type verkeersgegeven**	**inhoud?**
transmissie	tijdstip (begin, eind), datum nummer verzender nummer ontvanger locatie eindapparatuur (cel-ID) gebruikte protocol formaat	mogelijk
facturering	duur volume (omvang) soort dienst NAW-gegevens betaler	nee
dienstbeheer	NAW-gegevens gebruiker nummers van gebruiker	nee
toegevoegdewaardedienst	verfijnde locatiegegevens	mogelijk

Tabel 3a. Typologie van verkeersgegevens naar doel van verwerking (aanbieder)

Deze typologie bekijkt de verkeersgegevens vanuit de functionaliteit van de transporteur. Men kan echter ook een ander perspectief hanteren, namelijk voor welke functie de overheid verkeersgegevens zou willen verwerken. Volgens het WODC-onderzoek naar het gebruik van de telefoon- en Internettap in de opsporing, vraagt de politie vooral historische verkeersgegevens op.[128] Daarbij kunnen de volgende doelen worden onderscheiden:[129]

- voorfase van aftappen: onderzoeken welk nummer het best kan worden getapt (welk nummer wordt het meest gebruikt; is er capaciteit om de hoeveelheid communicatie uit te luisteren);
- opsporingsinformatie:
    - in kaart brengen van netwerken (wie belt met wie);
    - met wie stond het slachtoffer in contact;

[126] Art. 2 onder g Richtlijn 2002/58/EG.
[127] Merk op dat zelfgekozen emailadressen onder 'nummers van de gebruiker' vallen in tabel 3, maar alleen iets over de inhoud van communicatie vertellen als zij zijn gebruikt bij een concrete communicatie; ze vallen dus alleen in het grijze gebied als het een 'nummer verzender' betreft bij een transmissie, maar niet als het om 'nummers van de gebruiker' in de zin van het dienstbeheer gaat.
[128] Odinot e.a. 2012, p. 115.
[129] Vgl. ibid., p. 111-115.

    - met wie heeft een getuige contact gehad;
- bewijsinformatie, bijvoorbeeld:
    - vaststellen contact tussen verdachte en slachtoffer;
    - locatiegegevens.

Deze doelen zullen grotendeels overeenkomen met die van inlichtingen- en veiligheidsdiensten, met de kanttekening dat bewijsinformatie bij deze diensten geen rol speelt.

Voor de verschillende doelen zijn verschillende typen verkeersgegevens het meest relevant. Om te bekijken welke nummers het beste afgetapt kunnen worden en om netwerken in kaart te brengen, zijn voor nummergegevens en NAW-gegevens nodig, alsmede wellicht duur en omvang, gebruikte protocol en soort dienst. Deze laatste informatie is daarbij alleen op geaggregeerd niveau nodig: het zal niet nodig zijn om deze gegevens per afzonderlijke communicatie te weten te komen. Voor andersoortige opsporingsinformatie en voor bewijsdoeleinden zijn juist wel gegevens per afzonderlijke communicatie wenselijk, en daarbij kan het sneller voorkomen dat verkeersgegevens zicht bieden op de inhoud van communicatie. Dit kan worden vertaald in een volgende typologie:

doel van verwerking (overheid)	**type verkeersgegeven**	**inhoud?**
voorfase aftappen (op welk(e) nummer(s) is een tap wenselijk?) of netwerken in kaart brengen	nummer verzender nummer ontvanger gebruikte protocol (geaggregeerd) formaat (geaggregeerd) duur (geaggregeerd) volume (geaggregeerd) soort dienst (geaggregeerd) NAW-gegevens betaler NAW-gegevens gebruiker nummers van gebruiker	nee
contact slachtoffer, getuigen als opsporingsinformatie of bewijsinformatie	nummer verzender nummer ontvanger tijdstip (begin, eind), datum duur volume gebruikte protocol formaat soort dienst locatie eindapparatuur (cel-ID) verfijnde locatiegegevens	mogelijk

Tabel 3b. Typologie van verkeersgegevens naar doel van verwerking (overheid)

Feitelijk komt deze typologie neer op een simpel criterium: hangen verkeersgegevens samen met een concrete communicatiehandeling, of houden ze in meer algemene zin verband met gebruik van communicatiemiddelen? Gegevens die niet samenhangen met een concrete communicatiehandeling, zoals welke emailadressen iemand gebruikt of een geaggregeerd overzicht van hoe vaak iemand met een bepaald nummer belt, bieden geen zicht op inhoud van concrete communicatie. Gegevens die wel samenhangen met een concrete communicatiehandeling bieden mogelijk wel zicht op de inhoud van die specifieke communicatie.

De typologieën naar doel van de verwerking (tabel 3a en 3b) bieden enig houvast om verkeersgegevens van inhoud af te bakenen. Bepaalde categorieën verkeersgegevens kunnen worden uitgesloten van inhoud, zoals verkeersgegevens die worden verwerkt voor facturering of dienstbeheer, of limitatief opgesomde (en voor dit doel geaggregeerde) verkeersgegevens die de overheid nodig heeft voor het in kaart brengen van netwerken of in de voorfase van aftappen. Voor de overige categorieën biedt deze indeling evenwel geen afbakeningscriterium: het zal afhankelijk van de context en de precieze invulling zijn of de desbetreffende verkeersgegevens als inhoud zouden moeten worden behandeld. Dat komt omdat functionele typologieën te maken hebben met de functies die verkeersgegevens hebben voor de aanbieder of de overheid, maar geen onderscheid maken in de beschermwaardigheid van gegevens, zoals de eerdere

conceptuele typologie deed. Beschermwaardigheid van verkeersgegevens kan echter niet alleen worden bekeken vanuit een abstract-theoretisch perspectief ontleend aan de semiotiek, maar ook vanuit de ratio van bescherming van verkeersgegevens, wat leidt tot een teleologische typologie.

4.3. Een teleologische typologie

Fischer maakt een onderscheid in verkeersgegevens dat gebaseerd is op een verschil in potentiële privacygevoeligheid. Hij bouwt daarbij voort op het model van Bordewijk & Van Kaam dat vier typen communicatiepatronen onderscheidt:

1. *conversatie*: individueel geïnitieerd en inhoud afkomstig van een individu (bijvoorbeeld telefoongesprek);
2. *registratie*: geïnitieerd door een centrale instantie en inhoud afkomstig van een individu (bijvoorbeeld telemarketing);
3. *consultatie*: individueel geïnitieerd en inhoud afkomstig van een centrale instantie (bijvoorbeeld *video-on-demand*);
4. *allocutie*: geïnitieerd door een centrale instantie en inhoud afkomstig van een centrale instantie (bijvoorbeeld televisie-uitzending).

Volgens Fischer is bij conversatie en registratie qua privacygevoeligheid de inhoud belangrijker dan de verkeersgegevens. Bij consultatie en allocutie kantelt het perspectief: daar is de inhoud minder gevoelig, maar het feit dat een individu die inhoud tot zich neemt is wel potentieel privacygevoelig.[130] Eenzelfde kanteling vindt volgens Fischer plaats bij locatiegegevens: eenvoudige locatiegegevens zijn nodig voor het afwikkelen van mobiele telecommunicatie, waarbij de inhoud van het verkeer gevoeliger is dan de globale locatie, maar bij toegevoegdewaardediensten worden de verfijnde (veel preciezere) locatiegegevens potentieel privacygevoeliger dan de inhoud van de communicatie.[131] Aldus komt Fischer tot een onderscheidt in twee typen verkeersgegevens:

- 'Type I traffic data: regular traffic data. These are traffic data relating to the traffic patterns conversation and registration, except for any high-resolution location data;
- Type II traffic data: special traffic data relating to the traffic patterns consultation and allocution, plus any high-resolution location data.

Type II traffic data deserve more protection than Type I. Also, the scope of protection of Type I traffic data is a priori thinner than the communication content to which it relates.'[132]

Met andere woorden: Fischers type I-gegevens zijn a priori minder beschermwaardig dan inhoud van communicatie (hoewel ze in bijzondere gevallen wel ex post even of meer privacygevoelig kunnen blijken). Type II-gegevens zouden meer beschermd moeten worden dan type I-gegevens, waarbij Fischer overigens in het midden laat of het beschermingsniveau hetzelfde zou moeten zijn als dat van inhoud van communicatie of een sui generis-beschermingsniveau.

Arno Smits stelt ook een onderscheid voor in verkeersgegevens naar privacygevoeligheid. Hij kijkt daarbij primair naar surfgegevens. Volgens Smits is een IP-adres of domeinnaam (overheid.nl) vergelijkbaar met een klassiek adresgegeven en dus een verkeersgegeven, maar is een volledige URL privacygevoeliger en niet vergelijkbaar met het oude begrip verkeersgegeven. Daarom zou een scheiding gemaakt moeten worden tussen deze twee typen.[133] Ook Ekker verwijst naar een onderscheid in privacygevoeligheid. Omdat gegevens over mobiele communicatie privacygevoeliger zijn dan verkeersgegevens die samenhangen met vaste communicatie, 'kan men betogen dat sommige verkeersgegevens meer bescherming verdienen dan andere.'[134] Het gaat dan vooral om locatiegegevens, die bij mobiele telefonie privacygevoeliger zijn dan bij vaste telefonie. Het is daarom een mogelijkheid om locatiegegevens apart te behandelen, of om een onderscheid te maken tussen verkeersgegevens behorend bij mobiele telefonie en verkeersgegevens behorend bij vaste telefonie. Dat kan men uitbreiden met verkeersgegevens behorend bij Internet, waarbij de meeste grijze gebieden

[130] Fischer 2010, p. 36-38.
[131] Ibid., p. 38.
[132] Ibid., p. 36.
[133] Smits 2006, p. 397, 399.
[134] Ekker 2003, p. 45.

bestaan en die, vooral voor wat betreft surfgegevens, volgens een breed gedragen visie in de literatuur meer bescherming behoeven dan klassieke verkeersgegevens.

Hierbij moet worden aangetekend dat de auteurs die een onderscheid naar privacygevoeligheid voorstellen, geen criterium of operationalisering expliciteren op basis waarvan iemand kan bepalen wanneer een gegeven meer of minder privacygevoelig is. Het onderscheid is bij hen meer een intuïtief onderscheid dat aan de hand van voorbeelden wordt geïllustreerd. Voor de rechtspraktijk biedt dat wellicht weinig houvast, omdat een abstract geformuleerd onderscheid in privacygevoeligheid steeds moet worden toegepast op concrete gevallen. Wellicht kan men daarom aanknopen bij onderscheiden die elders in de wetgeving worden gehanteerd, zoals het onderscheid tussen 'gewone' persoonsgegevens en gevoelige persoonsgegevens,[135] of een onderscheid tussen het maken van een geringe inbreuk op de persoonlijke levenssfeer en het maken van een meer dan geringe inbreuk op de persoonlijke levenssfeer waarbij 'een min of meer volledig beeld wordt verkregen van bepaalde aspecten van iemands leven'.[136] De wetgever kan echter ook in de toelichting een nadere omschrijving geven van wat privacygevoeligheid inhoudt in de telecommunicatiesfeer, die in de rechtsontwikkeling via jurisprudentie dan verder kan uitkristalliseren, zoals dat normaliter gaat met open normen in het recht.

Hoe men ook precies het begrip privacygevoeligheid omschrijft of invult, de literatuur geeft aan dat vooral Internetgegevens en locatiegegevens als privacygevoelig worden beschouwd. Een typologie zou daarom kunnen zijn:

- type A: verkeersgegevens behorend bij post en telefonie, met uitzondering van locatiegegevens bij mobiele telefonie; dit zijn de klassieke verkeersgegevens die onder het bestaande beschermingsregime vallen;
- type B: locatiegegevens bij mobiele telefonie en verkeersgegevens behorend bij Internet; dit zijn nieuwe typen verkeersgegevens die meer juridische bescherming nodig hebben dan type A.

Belangrijk om op te merken is echter dat de genoemde auteurs pleiten voor een onderscheid tussen bepaalde typen verkeersgegevens, waarbij de meer privacygevoelige gegevens meer bescherming verdienen, vanuit een algemeen privacybelang. De argumentatie voor het onderscheid tussen type I en II, of type A en B, is niet ingegeven door het belang van het correspondentiegeheim als zodanig – de vrijheid om privé te communiceren zonder dat de overheid meeluistert. De teleologie in deze typologieën is dus het belang van privacy in het algemeen en niet per se het correspondentiegeheim in het bijzonder.

Toch kan de discussie over een onderscheid in verkeersgegevens naar privacygevoeligheid niet geheel tot artikel 10 Gw – het algemene privacyrecht – worden verengd. Ten eerste is dat zo omdat de discussie in de literatuur vaak in het kader van artikel 13 Gw wordt gevoerd, vanwege het substantiële verschil in de *checks and balances* in beide grondwetsartikelen. Artikel 10 Gw biedt in formele zin nauwelijks juridische bescherming, omdat de wetgever bij of krachtens de wet privacyinbreuken kan invoeren, waarbij de Grondwet geen eis stelt ten aanzien van eventueel toezicht. Dit in tegenstelling tot artikel 13 Gw, waarbij de wetgever alleen bij (maar niet krachtens) de wet inbreuken kan invoeren en waarbij de inbreuk voor een belangrijk deel onderworpen is aan rechterlijk toezicht. Dit levert een vanzelfsprekende druk op om verkeersgegevens onder de werking van artikel 13 Gw te brengen, vanwege de privacygevoeligheid die verkeersgegevens in het huidige communicatielandschap kenmerkt.

Ten tweede kan de discussie over beschermingsniveaus van verkeersgegevens niet verengd worden tot artikel 10 Gw, omdat er wel degelijk een samenhang bestaat tussen de privacygevoeligheid van verkeersgegevens en de ratio van het correspondentiegeheim: de wetenschap dat (privacygevoelige) verkeersgegevens als surfgegevens of locatiegegevens voor andere doelen dan communicatietransport worden gebruikt, zou burgers kunnen belemmeren om vrijelijk hun communicatiekeuzes te maken. Zij zouden bijvoorbeeld minder snel bepaalde informatie op Internet op zoeken of op bepaalde locaties hun telefoon aanzetten, omdat derden dan een onwenselijk scherp inzicht zouden kunnen krijgen in hun privégedrag. Om die reden past het in de systematiek van de privacygrondrechten om verkeersgegevens onder de werking van artikel 13 Gw te brengen,[137] en daarbij een onderscheid te maken binnen verkeersgegevens naar

[135] Zie art. 16 Wbp.
[136] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 26-27.
[137] Vgl. par. 2.2 en de eerste alinea van par. 2.4.

privacygevoeligheid. De minder gevoelige gegevens – afhankelijk van de gekozen typologie, type I of type A – zouden dan op een lager niveau worden beschermd dan de meer gevoelige gegevens – type II of type B. Deze laatste categorieën zouden dan, vanuit de ratio van het correspondentiegeheim en het mogelijk verkillend effect van kennisneming van deze gegevens op de privécommunicatievrijheid van burgers, aanspraak kunnen maken op hetzelfde beschermingsniveau als inhoud van communicatie.

4.4. Conclusie

In dit hoofdstuk zijn diverse typologieën van verkeersgegevens gepresenteerd die zouden kunnen helpen bij de beantwoording van de vraag welke verkeersgegevens onder de bescherming van artikel 13 Gw zouden moeten vallen gezien de ratio van het correspondentiegeheim. Hiermee is de derde onderzoeksvraag naar classificatie van de grijze gebieden beantwoord. Het blijkt dat er geen eenvoudig afbakeningscriterium is aan de hand waarvan een logische typologie kan worden geformuleerd die eenduidig verkeersgegevens indeelt in gegevens die niet en gegevens die wel dusdanig samenhangen met inhoud van communicatie dat zij onder artikel 13 Gw zouden moeten vallen. Dat viel ook te verwachten: als er wel een eenduidig en afdoende afbakeningscriterium zou zijn, dan zou dat in de literatuur al wel zijn geformuleerd en zou er geen diepteonderzoek nodig zijn geweest naar de afbakening tussen verkeersgegevens en inhoud.

Wat wel mogelijk blijkt, is om typen verkeersgegevens te ordenen aan de hand van bepaalde criteria, waarmee het afbakeningsprobleem wordt verkleind of in elk geval meer inzichtelijk wordt gemaakt. Zo kunnen verkeersgegevens worden ingedeeld naar de manier waarop zij mogelijk samenhangen met inhoud, volgens het semiotische onderscheid in soorten tekenrelaties. Verkeersgegevens die een afbeelding of diagram vormen van de inhoud of die indexicaal verwijzen naar inhoud, hebben over het algemeen een nauwer verband dan verkeersgegevens die metaforisch of symbolisch verwijzen naar inhoud. Dit biedt een zinvol materieel criterium om een scheidslijn tussen beschermingsniveaus van verkeersgegevens en inhoud te trekken. Het is wel een vrij abstract criterium dat veel interpretatie vergt. Bovendien leidt het tot een onderscheid binnen bepaalde categorieën verkeersgegevens, zoals telefoonnummers en emailadressen, dat weliswaar inhoudelijk hout snijdt maar ver afstaat van de juridische werkelijkheid waarin nummers en adressen als één categorie worden behandeld.

Een indeling naar het doel van de verwerking kan wel worden gebruikt om bestaande juridische categorieën verkeersgegevens te classificeren. Dat leidt tot twee mogelijke typologieën – een vanuit het perspectief van doelen van de aanbieder en een vanuit het perspectief van doelen van de overheid – waarbij bepaalde typen niet met inhoud samenhangen en dus als pure verkeersgegevens kunnen worden behandeld. Bij gebrek aan een materieel criterium kunnen de verkeersgegevens van de andere typen echter moeilijk worden beoordeeld.

Een derde mogelijkheid is om verkeersgegevens in te delen naar privacygevoeligheid, vanuit de gedachte dat artikel 13 Gw een bijzonder privacygrondrecht is en dus beoogt om de privacy van burgers te beschermen. In deze benadering gaat het dan niet zo zeer om het aanvullend beschermen van bepaalde categorieën verkeersgegevens omdat ze samenhangen met de inhoud, maar omdat ze privacygevoeliger zijn dan andere categorieën. Omdat de privacygevoeligheid van verkeersgegevens wel samenhangt met de ratio van het correspondentiegeheim – kennisneming ervan kan een verkillend effect hebben op de vrijheid om privé te communiceren – kunnen de meer privacygevoelige categorieën verkeersgegevens onder artikel 13 Gw worden beschermd, mogelijk op hetzelfde niveau als inhoud.

Omdat geen van de typologieën een ideale afbakening oplevert, is het nodig om nader te analyseren of een combinatie van criteria en typologieën mogelijk is die de voordelen van de diverse indelingen bundelt.

5. Synthese: de beschermwaardigheid van verkeersgegevens onder artikel 13 Gw

Uit de literatuur komt naar voren dat de ratio van het correspondentiegeheim is gelegen in de vrijheid om vertrouwelijk te kunnen communiceren. Die vrijheid impliceert dat artikel 13 Gw de vertrouwelijkheid van het communicatieproces beschermt, en het correspondentiegeheim zou dan ook de gegevens moeten beschermen die samenhangen met dat proces. Dat wil niet zeggen dat verkeersgegevens aanspraak zouden moeten maken op hetzelfde beschermingsniveau als inhoud, omdat er een zeker kwalitatief verschil kan bestaan tussen verkeersgegevens en inhoud, vergelijkbaar met het verschil tussen het correspondentiegeheim in ruime zin en dat in enge zin.

Zoals geconcludeerd in hoofdstuk 2 is de 'inhoud' van communicatie dat deel van de communicatie dat valt onder de verantwoordelijkheid van de verzender (en niet van de transporteur). Gelet op de ratio van bescherming door artikel 13 Gw gaat het niet alleen om de letterlijke en volledige inhoud, maar ook om gegevens die de strekking weergeven van (een deel van) de inhoud. Hierdoor ontstaat een afbakeningsprobleem: wanneer geven gegevens die primair onder de verantwoordelijkheid van de transporteur vallen (als samenhangend met het transport) voldoende zicht op de strekking van (een deel van) de inhoud van communicatie om aanspraak te kunnen maken op het beschermingsniveau van de inhoud van communicatie?

Zoals blijkt uit de analyse van de grijze gebieden[138] is dit een complexe vraag die zich niet makkelijk laat beantwoorden. Binnen de grijze gebieden vallen allerlei voorbeelden te geven van zowel gegevens die iets meer neigen naar pure verkeersgegevens als gegevens die iets meer neigen naar inhoud. De eenvoudigste oplossing voor dit afbakeningsprobleem is om, zoals Jan Smits aanbeveelt op basis van zijn technische analyse, verkeersgegevens integraal onder artikel 13 Gw te brengen en collectief te behandelen als inhoud.[139] Het collectief onderbrengen van verkeersgegevens onder inhoud voorkomt dat er steeds weer bij technische ontwikkelingen bepaald moet worden of bepaalde gegevens nu wel of niet voldoende zicht geven op de inhoud van communicatie om ze als inhoud te behandelen. Dat is een groot voordeel gezien de technische turbulentie die het telecommunicatielandschap, met steeds nieuwe applicaties en zich steeds ontwikkelende protocollen, kenmerkt.[140]

Hoewel er vanuit analytisch oogpunt veel voor die benadering te zeggen valt, kunnen er vanuit juridisch-praktisch en politiek perspectief bezwaren tegen worden gemaakt. De wetgeving en praktijk zijn eraan gewend geraakt om verkeersgegevens op redelijk laagdrempelige wijze te verwerken en om deze anders te behandelen dan inhoud. Het integraal onderbrengen van verkeersgegevens onder inhoud zou een systeembreuk in de lagere wetgeving betekenen. Daar is niets op tegen als die systeembreuk vanuit grondwettelijk oogpunt gewenst is, integendeel: de Grondwet moet leidend zijn voor lagere wetgeving en niet omgekeerd. Het is echter niet zeker dat het afschaffen van het onderscheid momenteel vanuit een grondwettelijke ratio aan de orde is. Het argument om verkeersgegevens integraal onder inhoud te scharen lijkt vooralsnog vooral gelegen in het praktische probleem een geschikt afbakeningscriterium en werkbare afbakeningsprocedure te formuleren, en niet zozeer in een intrinsieke ratio om alle verkeersgegevens op dezelfde wijze als communicatie-inhoud te behandelen. Er bestaat nog steeds, tot op zekere hoogte, een kwalitatief verschil tussen verkeersgegevens en inhoud, dat globaal gesproken gepaard gaat met een, tot op zekere hoogte, verschil in aanspraak op juridische bescherming. Met andere woorden, het afbakeningsprobleem zou vermoedelijk niet door het paardenmiddel van het compleet afschaffen van een onderscheid moeten worden opgelost.

---

[138] Zie hfd. 3 en vooral Smits 2013.

[139] Ibid. Zie ook Hes 2003, p. 18. Vgl. ook Asscher en Ekker 2003, p. 104: 'Zowel in de discussie over de technische aspecten van verkeersgegevens als in de juridische debatten worden vraagtekens geplaatst bij de wénselijkheid om nog onderscheid te maken tussen de inhoud van communicatie en de verkeersgegevens.'

[140] Smits 2013; Hes 2003, p. 18: 'Ook zou de dynamiek in de technologie kunnen leiden tot een continue herdefinitie van de scheidslijn tussen inhoud en verkeersgegevens en derhalve aan voortdurend "achterlopende" wetgeving.'

De vraag is echter wat dan wel een geschikt afbakeningscriterium is. Zoals in hoofdstuk 2 en 4 betoogd, is het primaire onderscheid gebaseerd op de vraag onder wiens verantwoordelijkheid de gegevens vallen:

- inhoud is datgene wat onder verantwoordelijkheid van de verzender valt;
- verkeersgegevens zijn gegevens die onder verantwoordelijkheid van de transporteur (als transporteur) vallen.

Sommige van de verkeersgegevens vallen weliswaar onder verantwoordelijkheid van de transporteur, maar kunnen de strekking weergeven van (een deel van) datgene wat valt onder de verantwoordelijkheid van de verzender. In dat geval zouden zij als inhoud moeten worden behandeld. Voor het bepalen van wanneer verkeersgegevens de strekking weergeven van (een deel van) de inhoud, kan in eerste instantie een negatieve benadering worden gevolgd. Het is mogelijk gegevens aan te wijzen die in elk geval niet (of nauwelijks) zicht geven op de strekking van communicatie.

Dat is in de eerste plaats het geval bij gegevens die niet samenhangen met een concrete communicatiehandeling, waaronder gebruikersgegevens en geaggregeerde verkeersgegevens vallen. Deze gegevens kunnen bijvoorbeeld worden gebruikt om netwerken van (potentiële) verdachten in kaart te brengen of om te bepalen welke telecommunicatienummers het beste kunnen worden afgetapt (zie typologie 3b in hfd. 4). Het omvat met name gegevens die veelal relevant zijn voor facturering of dienstbeheer in plaats van voor transmissie van een specifieke communicatie (zie typologie 3a in hfd. 4).

Voor wat betreft gegevens die wel samenhangen met een concrete communicatiehandeling, kunnen ten tweede ook gegevens worden uitgesloten die de 'klassieke' verkeersgegevens vormen waar het juridische beschermingsregime voor verkeersgegevens uit is voortgekomen: de verkeersgegevens behorend bij post en telefonie,[141] met uitzondering van locatiegegevens bij mobiele telefonie (een type verkeersgegeven dat historisch gezien niet bekend was bij de ontwikkeling van het juridische regime rond verkeersgegevens, en dat van een andere aard is dan klassieke adresgegevens). Weliswaar kunnen in sporadische uitzonderingsgevallen dit type 'klassieke' gegevens (wie belt wanneer met wie) ook zicht bieden op de strekking van de inhoud van communicatie (bijvoorbeeld als iemand het nummer 0906- 2569562 belt, wat een naamnummer is voor 0906-BLOWJOB), maar dat is zo zeldzaam dat deze categorie wel generiek als verkeersgegevens en niet als inhoud kan worden behandeld.

Hiermee is het probleemgebied in elk geval nader ingeperkt, namelijk tot verkeersgegevens behorend bij concrete communicatiehandelingen die samenhangen met Internet of locatiegegevens bij mobiele telefonie. Dit zijn gegevens waar de grijze gebieden het meest grijs zijn: of zo'n verkeersgegeven onder inhoud valt hangt erg af van het concrete gegeven (postzegelverzamelaar@aanbieder.nl biedt geen zicht op de strekking van een concreet bericht, jaikkomnaarpetersfeestje@yahoo.com biedt wel zicht op de vermoedelijke strekking van een concreet bericht) alsook van de context (bijvoorbeeld of de overheid het gegeven in verband kan brengen met andere gegevens die in samenhang zicht bieden op de inhoud van communicatie).

Voor dit probleemgebied zou de afbakening gezocht kunnen worden in de semiotische relatie tussen verkeersgegeven en inhoud. Een vuistregel is dat als het verkeersgegeven verwijst naar de inhoud als een afbeelding, een diagram, een index, een sterke metafoor of een sterk symbool, het als inhoud moet worden beschouwd; in de andere gevallen (een zwakke afbeelding, contextloze index, gewone metafoor of gewoon symbool) kan het als verkeersgegeven worden behandeld. Deze afbakening zou vanwege de contextspecificiteit eigenlijk op het niveau van concrete verkeersgegevens gemaakt moeten worden, maar dat zou een grote detaillering vergen van alle mogelijke subcategorieën van verkeersgegevens in het onderhavige probleemgebied. De wetgever is gewend te werken met globale categorieën verkeersgegevens, zoals 'adres', 'nummer' of 'tijdstip'. Het is in beginsel mogelijk om voor elk grijs gebied een meer categorische afweging te maken, afhankelijk van de vraag of de categorie verkeersgegeven *meestal* wel of *meestal* niet verband houdt met de strekking van communicatie. Zo biedt een zelfgekozen emailadres meestal geen zicht op de strekking van een concrete communicatie (het is meestal een symbool in plaats van een afbeelding van de vermoedelijke inhoud), terwijl een URL meestal wel direct verband houdt met de inhoud van communicatie (het is meestal een index, waarbij de koppeling met specifieke inhoud van een geconsulteerde webpagina te maken valt).

[141] Zie art. 100 lid 2-3 Sv-1926, zie daarover Koops 2002, p. 108-112.

Mogelijk blijft dan nog een restverzameling over van categorieën verkeersgegevens die even vaak wel als niet zicht bieden op de strekking van communicatie, maar die restverzameling is wellicht voldoende klein om op basis van een andersoortige belangenafweging een keuze te maken of de desbetreffende categorie verkeersgegeven als verkeersgegeven of als inhoud moet worden behandeld.

Samenvattend komt de hier beschreven afbakening neer op het volgende stroomschema:

1. Valt het gegeven onder verantwoordelijkheid van de communicatiepartner(s)?
   Zo ja → inhoud. Zo nee → verkeersgegeven maar mogelijk (ook) inhoud. Ga naar vraag 2.
2. Biedt het verkeersgegeven mogelijk zicht op de inhoud?
   Zo nee → verkeersgegeven. Zo ja → mogelijk inhoud. Ga naar vraag 3.
3. Houdt het verkeersgegeven verband met een concrete communicatiehandeling?
   Zo nee → verkeersgegeven. Zo ja → mogelijk inhoud. Ga naar vraag 4.
4. Is het een verkeersgegeven behorend bij telefonie (maar geen locatiegegeven)?
   Zo ja → verkeersgegeven. Zo nee → mogelijk inhoud. Ga naar vraag 5.
5. Heeft het verkeersgegeven een sterke relatie met de inhoud? Er is een sterke relatie als het verkeersgegeven semiotisch een afbeelding, diagram, index, sterke metafoor of een sterk symbool is van de inhoud.
   Zo ja → inhoud. Zo nee → verkeersgegeven.

De volgende tabel illustreert hoe de verschillende categorieën verkeersgegevens via dit stroomschema kunnen worden geclassificeerd.

antwoord **classificeringsvraag**	**ja**	**nee**
1. Valt het gegeven onder verantwoordelijkheid van de communicatiepartner(s)?	Inhoud sms-bericht emailonderwerpregel telefoonkeuzemenu URL van zoekmachine na "?": zoeken-op=grondwet	*Ga naar vraag 2.*
2. Biedt het verkeersgegeven mogelijk zicht op de inhoud?	*Ga naar vraag 3.*	Verkeersgegeven contextloos locatiegegeven mobiele telefoon URL van zoekmachine tot en met "?": http://www.google.com/search? toegewezen emailadres
3. Houdt het verkeersgegeven verband met een concrete communicatiehandeling?	*Ga naar vraag 4.*	Verkeersgegeven geaggregeerde verkeersgegevens
4. Is het een verkeersgegeven behorend bij post of telefonie (maar geen locatiegegeven)?	Verkeersgegeven *telefonie:* nummer verzender nummer ontvanger tijdstip (begin, eind), datum duur soort dienst *post:* adres verzender adres ontvanger datum volume soort dienst	*Ga naar vraag 5.*

antwoord **classificeringsvraag**	**ja**	**nee**
5. Heeft het verkeersgegeven een sterke relatie met de inhoud? Semiotisch: is het een afbeelding, diagram, index, sterke metafoor, sterk symbool?	Inhoud *afbeelding* [dit zijn gegevens die vrijwel altijd onder vraag 1 al als inhoud zijn gekwalificeerd, zoals emailonderwerpregel] *diagram* patroon van webaanmelding + emailbevestiging *sterke metafoor* presentmelding *index* URL *sterk symbool* contextrijk locatiegegeven	Verkeersgegeven *symbool* poortnummer Internetprotocol zelfgekozen emailadres contextarm locatiegegeven

Tabel 4. Stroomschema voor classificering van verkeersgegevens

Uit het schema blijkt dat URL's en locatiegegevens op diverse plaatsen terugkomen. Aangezien een URL uiteindelijk als een index fungeert en daarmee over het algemeen gekoppeld kan worden aan de inhoud van een webpagina, kunnen URL's integraal als inhoud worden gekwalificeerd. Locatiegegevens blijven echter afhankelijk van de context.

De classificatie kan vervolgens ook worden gegroepeerd naar verschillende soorten communicatie (zoals de Wet bewaarplicht telecommunicatiegegevens verschillende categorieën hanteert van telefonie, email en Internet[142]). Op basis van de hierboven gegeven argumentatie en toepassing van het stroomschema, zou ik de verschillende typen gegevens als volgt classificeren als inhoud dan wel als verkeersgegevens:

beschermingsregime **soorten communicatie**	**inhoud**	**verkeersgegevens**
post		adres verzender adres ontvanger datum volume soort dienst
telefonie	sms-bericht telefoonkeuzemenu (toonkiezen) contextrijk locatiegegeven	nummer verzender nummer ontvanger tijdstip (begin, eind), datum duur soort dienst contextloos of contextarm locatiegegeven
Internet: email	emailonderwerpregel	emailadres verzender emailadres ontvanger tijdstip (begin, eind), datum volume
Internet: overig	URL's patroon van webaanmelding + emailbevestiging presentmelding	poortnummer Internetprotocol geaggregeerde verkeersgegevens

Tabel 5. Classificatie van typen verkeersgegevens naar beschermingsregime

[142] Zie noot 124.

Hiermee is een antwoord geformuleerd op de vierde onderzoeksvraag, namelijk welke typen verkeersgegevens beschermwaardig zijn onder artikel 13 Gw omdat zij 'inhoud' betreffen: dat geldt voor de gegevens in de kolom 'inhoud'.[143] De tabel moet echter niet worden gezien als een uitputtende opsomming, noch als een definitief antwoord. Met name voor wat betreft Internet zijn er vele soorten gegevens die moeilijk te vangen zijn onder simpele noemers; daarvoor zijn de protocollen en applicaties te divers.[144] De tabel geeft ook geen definitief antwoord omdat er verschillen kunnen ontstaan door de combinatie van gegevens; wanneer men alle verkeersgegevens heeft behorend bij iemands Internetgebruik over een periode van een paar uur 'is het vrij gemakkelijk geworden de inhoud van al die verschillende (internet)activiteiten te duiden, zonder daadwerkelijk de inhoud te kennen'.[145] Ook kan de combinatie van verkeersgegevens uit de rechterkolom – die dus in beginsel niet onder het beschermingsregime van inhoud vallen – met gegevens uit andere bronnen een dusdanige context opleveren dat de verkeersgegevens dan wel de inhoud van communicatie weerspiegelen.[146] Daarnaast moet ook onder ogen worden gezien dat door convergentie langzamerhand het onderscheid verdwijnt tussen telefonie, email en (overig) Internet.[147] Om deze redenen is nog een nadere reflectie nodig.

[143] Daarbij moet worden aangetekend dat er goede systematische redenen zijn om alle verkeersgegevens onder artikel 13 Gw te brengen, dus ook die in de rechterkolom van Tabel 5. Die kolom betreft dan verkeersgegevens die binnen artikel 13 Gw met een lichtere beperkingsclausule zouden kunnen worden beschermd.
[144] Zie Smits 2013.
[145] Ibid., p. 39.
[146] Zie par. 3.11.
[147] Zie Smits 2013, o.a. bijlage 4.

6. Reflectie

6.1. Eerste reflectie: afbakeningscriteria en onderscheid telefonie, email, Internet

In het voorgaande is een inhoudelijke analyse gegeven van de afbakening tussen verkeersgegevens en inhoud. Dat heeft een tamelijk complex beeld opgeleverd. Hoewel het mogelijk is om verkeersgegevens volgens het in het vorige hoofdstuk gepresenteerde stroomschema te classificeren (zoals in Tabel 5 is gedaan), is het de vraag of het juridisch en technisch haalbaar is om een dergelijk classificeringsmodel in wetgeving en praktijk te hanteren. Daarom luidt het tweede onderdeel van de hoofdonderzoeksvraag: in hoeverre zijn de beschermwaardige typen verkeersgegevens juridisch af te bakenen op een manier die verenigbaar is met de technische realiteit?

In beginsel is een tweeledig afbakeningscriterium te formuleren dat juridisch voldoende abstractieniveau heeft en dat inhoudelijk goed werkt om de kern van het onderscheid tussen inhoud en verkeersgegevens te duiden. Het **hoofdcriterium** is **onder wiens verantwoordelijkheid de gegevens vallen**: **inhoud is datgene wat onder verantwoordelijkheid van de verzender valt**; verkeersgegevens zijn gegevens die onder verantwoordelijkheid van de transporteur (als transporteur) vallen. Het **nevencriterium** is dat **verkeersgegevens** die (juridisch-)technisch onder het begrip verkeersgegevens vallen, onder artikel 13 Gw **als inhoud moeten worden behandeld wanneer zij de strekking weergeven van (een deel van) datgene wat valt onder de verantwoordelijkheid van de verzender**.

De operationalisering van dit laatste criterium levert echter complicaties op. Zoals hoofdstuk 5 laat zien, zijn er diverse argumentatiestappen nodig om grijze gebieden volgens dit criterium uiteindelijk in te delen naar het beschermingsregime van inhoud of van verkeersgegevens. Enig houvast kan worden gevonden in de semiotische duiding van de manier waarop verkeersgegevens samenhangen met inhoud. Dat is evenwel een vrij abstracte exercitie die de nodige interpretatie vergt, en bovendien contextafhankelijk blijkt. De typen verkeersgegevens waarmee de wetgever tot nu toe gewoon is te werken – zoals 'nummer', 'adres' of 'cel-ID' – kennen in de technische werkelijkheid allerlei verschijningsvormen, waardoor deze soms meer en soms minder de strekking van communicatie-inhoud blootgeven. Met name bij Internetcommunicatie ontstaat een zeer complex beeld van wat verkeersgegevens wel of niet over communicatie-inhoud kunnen zeggen.

Wil men verkeersgegevens juridisch afbakenen van inhoud op een manier die verenigbaar is met de technische realiteit, dan suggereert de technische analyse van Jan Smits voor wat betreft Internetcommunicatie dat voor door de dynamiek en diversiteit van Internetprotocollen, verkeersgegevens niet zinvol meer te scheiden zijn van inhoud.[148] Om het correspondentiegeheim niet uit te hollen, zouden daarom alle Internetgerelateerde verkeersgegevens onder het beschermingsregime van communicatie-inhoud moeten vallen. Voor (klassieke) telefonie valt de scheiding echter wel eenvoudiger te maken, evenals vermoedelijk voor email. Het afbakeningsprobleem zou daarom op dit moment opgelost kunnen worden door het bovengenoemde tweeledige criterium te hanteren, waarbij het nevencriterium als volgt wordt toegepast:

- verkeersgegevens behorend bij telefonie die onder het beschermingsregime van verkeersgegevens vallen worden limitatief opgesomd (zoals in de rechterkolom in Tabel 5); de overige telefoniegerelateerde verkeersgegevens vallen onder het beschermingsregime van inhoud;
    - locatiegegevens bij mobiele telefonie vormen een sui generis-categorie; hiervoor dient de wetgever een zelfstandige keuze te maken, omdat het voor deze te contextafhankelijk is om te bepalen of zij de strekking van communicatie-inhoud weergeven;

[148] Ibid., p. 38-39.

- verkeersgegevens behorend bij email die onder het beschermingsregime van verkeersgegevens vallen worden limitatief opgesomd (zoals in de rechterkolom in Tabel 5); de overige emailgerelateerde verkeersgegevens vallen onder het beschermingsregime van inhoud;
- verkeersgegevens behorend bij Internet (met uitzondering van email) vallen onder het beschermingsregime van inhoud.

6.2. Nadere reflectie: alles is Internet, (dus) alles wordt inhoud

Het is de vraag of de in de vorige subparagraaf geschetste benadering voldoende duurzaam is. De Grondwet zelf hoeft niet tot in detail de afbakening van verkeersgegevens en inhoud te duiden; de tekst van artikel 13 Gw zou vermoedelijk alleen de term 'post- en telecommunicatiegeheim' bevatten en de toelichting zou op hoofdlijnen een afbakening langs bovenstaande lijnen kunnen bevatten. De toelichting bij het Grondwetsartikel is echter wel leidend voor de interpretatie van het grondrecht in de toekomst. Nu kan het makkelijk een jaar of tien kan duren voordat een nieuwe grondwetsbepaling in werking treedt[149] en men zou willen dat de bepaling vervolgens ook ten minste enkele decennia meegaat. Daarom moet de toelichting bij de grondwetswijziging voldoende helder zijn om voor de komende decennia de wetgever (en wie weet op termijn ook de rechter) richting te geven aan wat op welk niveau beschermwaardig is aan telecommunicatie.

Voor een begrip van wat 'enkele decennia' betekent in termen van technologische ontwikkeling, is het zinvol te bedenken hoe de ontwikkeling van telecommunicatie in de afgelopen decennia heeft plaatsgevonden. Sinds de lancering van het wereldwijde web in 1991 heeft Internetcommunicatie fundamentele transformaties ondergaan, met onder andere de opkomst van sociale media / web 2.0, mobiel Internet, cloud computing en allerlei toepassingen die door breedbandverbindingen en eindgebruikersoftware (*peer-to-peer*-programma's, apps) mogelijk zijn gemaakt. Deze transformaties waren 25 jaar geleden moeilijk te voorzien, en de gevolgen ervan voor hoe telecommunicatie plaatsvindt waren in geen enkel opzicht te overzien. Het valt nu niet te voorzien hoe de ontwikkeling van het Internet zich in de komende dertig jaar zal doorzetten, maar het valt wel te voorspellen dat er zich onvoorspelbare transformaties zullen voordoen. En dit alles gaat gepaard met een aanzienlijke technologische turbulentie in de protocollen en standaarden die met de ontwikkelingen in infrastructuur en applicaties gemoeid zullen zijn.

Het is zeer de vraag of een indeling in telefonie, email en "overig Internet" hout snijdt. Het onderscheid is nu al aan het vervagen en zal op de middellange termijn weinig of geen relevantie meer hebben. De klassieke telefonie-infrastructuur van circuitgeschakelde telefoonnetten en GPS-mobiele telefonie raken snel uitgefaseerd; vrijwel alle telefonie is tegenwoordig al pakketgeschakeld. Waar wetgeving nu categorieën hanteert van 'telefonie over een vast of mobiel netwerk' en 'internettelefonie', wordt miskend dat vaste en mobiele telefonie nu ook al grotendeels via pakketgeschakelde infrastructuren worden afgehandeld. Daarbij is het de vraag hoe het begrip 'telefonie' in de toekomst geduid moet worden.[150] Gesprekken worden nu al via verschillende protocollen via Internet getransporteerd en het lijkt niet erg zinvol om verschillende protocollen in te delen in 'klassieke' telefonie of 'Internettelefonie' afhankelijk van waar ze het meest op lijken. Daarbij is het de vraag wat de ratio is van aparte categorieën 'telefonie' of 'email', als communicatie via Internet allerlei vormen kan aannemen, met niet alleen verschillende protocollen maar ook uiteenlopende functionaliteiten (allerlei vormen van mens-mens-, mens-machine- en machine-machine-communicatie) en formaten (tekst, spraak, beeld, multimedia). 'Email' is geen intrinsieke categorie vanuit de ratio van het correspondentiegeheim, nu een sms-bericht en een chatbericht in een online spel dezelfde functionaliteit hebben voor gebruikers als een korte email. 'Telefonie' is geen intrinsieke categorie vanuit de ratio van het correspondentiegeheim, nu 'telefoons' computers zijn geworden waarmee je even goed 'klassiek' kunt bellen ('mobiele telefonie') als Skypen ('Internettelefonie') of Whatsappen ('Internettelefonie' of overig 'Internet'?), en tegelijkertijd telefoongesprekken in het sociale verkeer vaak een uitwisselbare functie hebben met andere vormen van communicatie (als chatten, sms'en en Facebooken).

[149] Vergelijk de vorige wijziging: de tekst van het huidige art. 13 Gw werd eind 1976 door de Tweede Kamer vastgesteld en trad grotendeels in 1988 in werking.
[150] Zie ook Smits 2013, p. 39.

Kortom, nu alle communicatie pakketgeschakeld wordt en daarmee van Internetprotocollen gebruik maakt, heeft een categorie 'Internetcommunicatie' geen onderscheidende waarde meer. De categorieën 'telefonie' en 'email' hebben geen eeuwigheidswaarde wanneer alles over Internet gaat en allerlei communicatievormen in elkaar overvloeien. Wanneer alles over Internet gaat, in complexe en uitwisselbare patronen, is de consequentie ook dat alles wat met telecommunicatie te maken heeft – vanuit de in hoofdstuk 5 geschetste argumentatie – inhoud wordt.

Misschien zouden we dan ook moeten constateren dat het begrip 'verkeersgegevens' zijn langste tijd gehad heeft. In de historische ontwikkeling van telecommunicatie zijn gegevens die nodig zijn voor het transport van berichten op een zeker moment 'losgekomen' van de boodschap, waardoor ze ook voor andere doeleinden dan enkel transport gebruikt konden worden.[151] Met de komst van mobiele telefonie en vooral Internet zijn er steeds nieuwe soorten verkeersgegevens bijgekomen, die op complexe manieren samenhangen met het berichtverkeer. Bij Internetcommunicatie valt weliswaar nog wel een conceptueel onderscheid te maken tussen verkeersgegevens en de inhoud van communicatie, maar dat conceptuele onderscheid verliest sterk aan relevantie als het gaat om het secundaire gebruik voor bijvoorbeeld marketing- of opsporingsdoeleinden (naast het pure transport) van de gegevens. Verkeersgegevens zijn dermate verknoopt met communicatiepatronen, dat het vaak mogelijk is dat kennis van de verkeersgegevens gepaard gaat met kennis van de strekking van wat er wordt gecommuniceerd.

De conclusie zou dan ook kunnen zijn dat, wanneer de categorieën 'telefonie' en 'email' achterhaald raken nu alle communicatie in complexe patronen en met een grote diversiteit aan applicaties en protocollen over Internet wordt getransporteerd, alle communicatie Internetcommunicatie is. Vanuit de hiervoor genoemde redenering dat verkeersgegevens behorend bij Internet als inhoud moeten worden beschermd, is dan de conclusie dat verkeersgegevens en inhoud altijd samenvallen vanuit de ratio van het correspondentiegeheim.

Wanneer het onderscheid tussen verkeersgegevens en inhoud van communicatie wegvalt in de wolk van Internetcommunicatie, blijft overigens wel een ander onderscheid staan dat gebruikt zou kunnen worden om de reikwijdte van het correspondentiegeheim te omschrijven. Dat is een onderscheid tussen communicatiegerelateerde gegevens (inhoud en verkeersgegevens) en gebruikersgegevens.[152] Communicatiegerelateerde gegevens zijn gegevens die samenhangen met concrete communicatiehandelingen. Deze raken de vrijheid om vertrouwelijk te kunnen communiceren en zouden daarom integraal onder artikel 13 Gw moeten vallen. Gebruikersgegevens zijn gegevens over iemands telecommunicatiegebruik in meer algemene zin, die niet samenhangen met een concrete communicatie; het zijn gegevens die iets zeggen over de gebruiker in plaats van over de communicatie. Daaronder vallen de identificerende gegevens die op basis van artikel 126na/ua/zi Sv kunnen worden gevorderd,[153]zoals NAW-gegevens, de soorten diensten en de telefoonnummers en emailadressen die iemand in gebruik heeft, alsook factuurgegevens. Vaste IP-adressen zijn vergelijkbaar met klassieke adresgegevens en zijn daarom ook gebruikersgegevens; dynamische IP-adressen kunnen echter dermate snel wisselen (ook binnen enkele minuten) dat zij sneller met concrete communicatiehandelingen in verband kunnen worden gebracht, zodat dynamische IP-adressen eerder als verkeersgegevens (en dus communicatiegerelateerde gegevens) zouden moeten

[151] Zie ibid., hoofdstuk 3.

[152] Dit onderscheid sluit aan op de functionele typologie naar doel van de verwerking (vanuit het aanbiedersperspectief), zie tabel 3b in par. 4.2. Gebruikersgegevens kunnen worden gezien als de gegevens die worden gegenereerd en verwerkt voor facturering en dienstbeheer, terwijl communicatiegerelateerde gegevens de gegevens zijn die worden gegenereerd en verwerkt voor transmissie van communicatie of voor toegevoegdewaardediensten.

[153] Art. 126na Sv geeft (evenals de parallelle artikelen 126ua en 126zi Sv) opsporingsambtenaren de bevoegdheid om 'gegevens te verstrekken terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst' te vorderen. Merk op dat gebruikersgegevens ook kunnen worden gevorderd op basis van art. 126n/u/zh Sv, de bevoegdheid die gemakshalve vaak wordt aangeduid als de bevoegdheid tot het vorderen van verkeersgegevens. Die aanduiding is niet helemaal correct, omdat art. 126n/u/zh zowel verkeersgegevens als gebruikersgegevens omvat ('een vordering (…) gegevens te verstrekken over een gebruiker van een communicatiedienst [oftewel gebruikersgegevens, BJK] en het communicatieverkeer met betrekking tot die gebruiker [oftewel verkeersgegevens, BJK]'). Omdat bij een vordering verkeersgegevens justitie ook bijna altijd de gebruikersgegevens nodig heeft, zijn deze twee categorieën samengenomen in één artikel.

worden beschouwd dan als gebruikersgegevens.[154] Naast de identificerende en factuurgegevens zouden ook geaggregeerde verkeersgegevens (welk volume wordt gebruikt over periode X door aansluiting Y? met welke telefoonnummers heeft telefoonnummer A contact over periode X?) onder het begrip 'gebruikersgegevens' kunnen worden geschaard, omdat door de aggregatie de koppeling met concrete communicatiehandelingen verdwijnt.[155] Deze gegevens raken de vrijheid vertrouwelijk te communiceren niet of nauwelijks, omdat ze niet samenhangen met concrete communicatiehandelingen en dus niet met specifieke keuzes om gebruik te maken van een communicatiemiddel. Daarom vallen gebruikersgegevens niet onder de reikwijdte van artikel 13 Gw. Een onderscheid tussen communicatiegerelateerde gegevens (waaronder zowel inhoud als verkeersgegevens vallen) en gebruikersgegevens zou voor de langere termijn een bruikbaarder afbakeningscriterium kunnen bieden dan een onderscheid tussen (niet inhoudgerelateerde) verkeersgegevens en inhoud van communicatie.

6.3. Nog nadere reflectie: waarom communicatie(inhoud) beschermen?

De reflectie zou nog een stap verder moeten gaan. Dit rapport bevat, conform de opdracht, een zoektocht naar een antwoord op de vraag wanneer verkeersgegevens onder artikel 13 Gw beschermd zouden moeten worden omdat zij inhoud van communicatie betreffen. Ik weet niet zeker of dat de meest relevante vraag is die de grondwetgever zich zou moeten stellen vanuit het perspectief van het wenselijke grondwettelijke beschermingsniveau van verkeersgegevens of, in meer algemene zin, van communicatiegerelateerde gegevens. De analyse in dit rapport en in de aanpalende technische analyse laat namelijk zien dat verkeersgegevens niet alleen vaak – in grotere of kleinere mate – verknoopt zijn met inhoud van communicatie, maar vooral dat het sterk contextafhankelijk is welk inzicht verkeersgegevens bieden in het communicatiegedrag van burgers. Het maakt niet alleen uit welke infrastructuur en welke protocollen er worden gebruikt, en dus welke typen verkeersgegevens precies worden verwerkt, maar vooral ook welke hoeveelheid gegevens iemand beschikbaar heeft om analyses op los te laten. En, zoals in de literatuur al vaker is betoogd, die analyses zijn inmiddels niet meer primair privacygevoelig omdat zij inzicht bieden in wat er precies wordt gecommuniceerd, maar omdat zij inzicht bieden in communicatiegedrag en vooral ook in gedragspatronen in het algemeen.

De consequentie van deze argumentatie is niet alleen dat verkeersgegevens een sterk niveau van juridische bescherming behoeven omdat zij, met name als zij over een bepaalde periode en voor meerdere communicatiemiddelen beschikbaar zijn, een scherp inzicht kunnen bieden in de persoonlijke levenssfeer van burgers. De consequentie is ook dat de noodzaak van bescherming van *inhoud* van communicatie ten opzichte van andere aspecten van communicatie – en van het persoonlijke leven in het digitale tijdperk in het algemeen – opnieuw doordenking behoeft. In de negentiende eeuw was er een bijzondere reden om aan de overheid als postvervoerder toevertrouwde brieven te beschermen tegen kennisneming door de overheid. In de twintigste eeuw lag het voor de hand om deze bescherming te extrapoleren naar telefonie (de telegrafie laat ik even buiten beschouwing), omdat naast de brief de telefoon het enige middel was waarmee burgers op afstand onderling vertrouwelijk contacten konden onderhouden en het daarbij onwenselijk was dat de overheid zo maar zou kunnen meeluisteren. In de eenentwintigste eeuw lijkt het voor de hand te liggen deze bescherming van inhoud van communicatie nu op dezelfde manier door te trekken naar Internetcommunicatie.

De ontwikkeling van Internetcommunicatie moet echter wel in perspectief worden geplaatst. Ten eerste is de functie van Internetcommunicatie veel uitgebreider en diverser dan communicatie via brief of telefoon ooit geweest is. Het gaat lang niet meer alleen om het communiceren met andere mensen of instanties, maar ook om het opslaan in de cloud van

[154] Vgl. BVerfG 24 januari 2012, 1 BvR 1299/05 (beschikbaar op http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html), §116, waarin het Duitse constitutioneel hof bepaalde dat dynamische IP-adressen onder de reikwijdte van het Duitse correspondentiegeheim vallen (dat zowel inhoud als verkeersgegevens beschermt), hetzij omdat ze nauw met concrete telecommunicatiehandelingen verbonden zijn, hetzij omdat de aanbieder voor de identificatie van een specifiek dynamisch IP-adres de daarbijbehorende verbindingsdata moet inzien en daarmee raakt aan concrete communicatiehandelingen.

[155] Daarbij is wel van belang dat de aggregatie dusdanig moet zijn dat de geaggregeerde gegevens niet meer terug te herleiden zijn tot concrete communicatiehandelingen, ook niet als de geaggregeerde gegevens in verband worden gebracht met andere gegevens die de overheid tot haar beschikking heeft of kan krijgen.

materiaal (muziek, boeken, foto's, documenten) dat vroeger in de beschermde muren van het huis lag opgeslagen. Het gaat ook om communicatie van sensoren of apparaten die via het Internet der dingen aan huis of lichaam zijn verbonden. Ten tweede is de hoeveelheid communicatie geëxplodeerd. Waar men vroeger per dag hooguit enkele brieven schreef en enkele telefoongesprekken voerde, worden nu honderden of duizenden communicatiehandelingen verricht – elke handeling op het web genereert berichtentransport. Ten derde betekent de ontwikkeling van *data mining* en profilering dat er uit grote hoeveelheden data allerlei verbanden kunnen worden afgeleid. De combinatie van deze drie aspecten betekent dat Internetcommunicatie steeds meer en steeds indringender inzicht biedt in de persoonlijke levenssfeer, ook zonder dat kennis wordt genomen van de *inhoud* van al die communicatie.

Daar komt bij dat burgers kwetsbaar zijn geworden nu we in een tijdperk komen waarin de locatie waar gegevens opgeslagen liggen, irrelevant wordt.[156] Gegevens die men opslaat in de cloud (zonder dat men deze deelt met anderen) zijn kwetsbaarder voor kennisneming door anderen dan gegevens die men thuis opslaat. Het is in dat licht begrijpelijk dat het wetsontwerp-2012 voorstelt om ook cloud-opslag onder het correspondentiegeheim te brengen,[157] maar conceptueel gezien is een cloud-opslagdienst geen nieuwe vorm van telecommunicatie (relationele privacy) maar een nieuwe vorm van materiaalopslag (ruimtelijke privacy). Het zou daarom, vanuit de ratio van de verschillende dimensies van privacybescherming, eerder passen om het huisrecht (art. 12 Gw) te actualiseren tot een meer locatieonafhankelijk, digitaal 'huis'recht dat ook extern opgeslagen maar vanuit het huis beschikbare gegevens beschermt die men van oudsher binnen het huis bewaarde.

De kwetsbaarheid voor kennisneming door anderen van vertrouwelijke gegevens in het 'locatieloze' tijdperk uit zich op vergelijkbare wijze ook in draagbare computers (laptops, tablets, smartphones) waarop men grote hoeveelheden gegevens meedraagt die van oudsher alleen of vooral thuis werden bewaard. Er bestaat een groot verschil in rechtsbescherming voor burgers tegenover kennisneming door de overheid van gegevens die zijn opgeslagen op hun computer, afhankelijk van het feit of de computer in het huis staat (art. 97/110 j° 125i Sv) of op een andere plaats dan een woning die wordt doorzocht (art. 96c j° 125i Sv), of in een auto ligt die door de politie wordt onderzocht (art. 96b j° 125i Sv), dan wel door iemand bij zich wordt gedragen wanneer hij wordt aangehouden (art. 95 Sv). In de laatste twee gevallen mag elke politieambtenaar de computer in beslag nemen en onderzoeken, terwijl bij de woning dat alleen is toegestaan met toestemming van de rechter-commissaris. Het is sterk de vraag of een dergelijk verschil in rechtsbescherming van computergegevens nog gerechtvaardigd is in het mobiele tijdperk.

Nu is het vraagstuk van digitale kwetsbaarheid als zodanig niet het onderwerp van het huidige rapport, maar de uitstap naar opgeslagen gegevens toont aan dat waar vroeger gegevensopslag niet als bijzondere categorie expliciet hoefde te worden beschermd omdat het van nature grotendeels onder het huisrecht viel, gegevensopslag in het huidige mobiele en Internettijdperk niet langer onder het (huidige) huisrecht valt, waardoor een lacune in de rechtsbescherming is ontstaan.

Het feit dat Internetcommunicatie een steeds indringender inzicht biedt in de persoonlijke levenssfeer ook zonder kennisneming van inhoud, en het feit dat naast communicatie ook gegevensopslag vragen oproept over grondwettelijke bescherming, betekenen dat de grondwetgever zich moet afvragen of er nog voldoende reden is om inhoud van communicatie als een zelfstandige categorie met meer egards te behandelen dan andere vormen van privacygevoelige gegevens in het digitale tijdperk. Is voor de komende decennia de verbijzondering van privacy in bescherming van lichaam, huis en communicatie(inhoud) nog wel de meest voor de hand liggende indeling als we kijken naar de verknooptheid van Internet met het menselijk gedrag in al zijn facetten? Zijn de meest bijzondere bedreigingen voor de burger nog steeds dat de overheid fysiek het lichaam aantast, fysiek het huis binnendringt of de inhoud van vertrouwelijke communicatie beluistert?

[156] Koops e.a. 2012b.

[157] Door de keuze voor een telecommunicatiegeheim 'verkrijgen ook e-mail, communicatie via de sociale media, *opslag van persoonlijke bestanden in de 'cloud'* en de zoekvraag om informatie op internet via een zoekmachine bescherming onder artikel 13'. Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 8 (cursivering toegevoegd).

Internetcommunicatie is niet langer een fenomeen dat zich uitsluitend in de relationele privacy van het correspondentiegeheim laat vangen; het is verknoopt met alle aspecten van wat burgers zijn en doen. Voor de kortere termijn heeft het wellicht nog zin om communicatie-inhoud – met inbegrip van verkeersgegevens die nauw verband houden met die inhoud – bijzondere bescherming te bieden ten opzichte van andere vormen van digitale kwetsbaarheid. Voor de langere termijn – en dat is een termijn die past bij het perspectief van de grondwetgever – lijkt het mij echter ook noodzakelijk om de systematiek van de privacygrondrechten over de hele linie opnieuw te doordenken, om effectief tegenwicht te bieden aan alle nieuwe vormen waarin de overheid zicht kan krijgen op de persoonlijke levenssfeer van burgers.

7. Samenvatting en conclusies

In dit rapport staat de volgende vraag centraal: welke typen verkeersgegevens moeten juridisch beschermwaardig worden geacht onder artikel 13 Gw, gelet op de ratio en functie van het correspondentiegeheim (zoals ik artikel 13 Gw in dit rapport aanduid), en in hoeverre zijn deze typen juridisch af te bakenen op een manier die verenigbaar is met de technische realiteit? Bij de beantwoording van deze vraag is, vanuit de nadruk die in het wetsontwerp-2012 ligt op de inhoud van communicatie als het te beschermen object onder artikel 13, vooral gekeken of het mogelijk is om een geschikte afbakening te ontwerpen tussen verkeersgegevens en inhoud.

Uit de literatuur komt naar voren dat de ratio van het correspondentiegeheim is gelegen in de vrijheid om vertrouwelijk te kunnen communiceren. Deze ratio wordt in de literatuur op een meer consistente manier beargumenteerd en doorgetrokken dan in de wetgevingsvoorstellen van de afgelopen decennia. Deze voorstellen stellen op hoofdlijnen dat het correspondentiegeheim de vertrouwelijkheid van communicatie beschermt (en daarmee beperkt is tot de inhoud van communicatie) maar bevatten ook regelmatig formuleringen die samenhangen met de vrijheid om vertrouwelijk te kunnen communiceren (en daarmee de vertrouwelijkheid van het communicatieproces in bredere zin aanduiden). Het valt daarom aan te bevelen dat de grondwetgever bij een nieuw wetsvoorstel een meer systematische uitwerking geeft van wat volgens hem de ratio van het correspondentiegeheim is in relatie tot de inhoud van communicatie en het communicatieproces in bredere zin.

Los van de vraag of verkeersgegevens, als onderdeel van het communicatieproces, als zodanig wel of niet beschermwaardig onder artikel 13 Gw worden geacht, is de vraag wat er precies onder ‘verkeersgegevens’ en ‘inhoud’ moet worden verstaan. Onder de ‘inhoud’ van communicatie kan worden verstaan dat deel van de communicatie dat valt onder de verantwoordelijkheid van de verzender of ontvanger (en niet van de transporteur). Verkeersgegevens zijn gegevens die vallen onder de verantwoordelijkheid van de transporteur (als transporteur). Gelet op de ratio van bescherming door artikel 13 Gw vallen onder inhoud ook (verkeers)gegevens die de strekking weergeven van (een deel van) datgene wat valt onder de verantwoordelijkheid van de verzender of ontvanger.

Uit de literatuur en uit de aan dit rapport aanpalende technische analyse van Jan Smits komen diverse grijze gebieden naar voren tussen verkeersgegevens en inhoud. Sommige van deze grijze gebieden betreffen gegevens die technisch gesproken als verkeersgegevens kunnen worden gekwalificeerd, maar die duidelijk onder de verantwoordelijkheid van de verzender of ontvanger vallen en dus inhoud betreffen (sms-bericht, emailonderwerpregel). Bij de meeste grijze gebieden gaat het echter om gegevens die (deels) onder de verantwoordelijkheid van de transporteur vallen, maar die in meer of minder sterke mate zicht bieden op de (strekking van de) inhoud van communicatie. Soms bestaat er een sterk of rechtstreeks verband met inhoud (bijvoorbeeld bij surfgegevens), vaak gaat het om een zwakker of indirecter verband (bijvoorbeeld bij emailadressen, informatienummers of poortnummers). Soms kan echter uit deze laatste gegevens ook de strekking van communicatie worden afgeleid, zeker als verkeersgegevens over lange tijd beschikbaar zijn en/of gecombineerd worden met andere gegevens.

Vallen de gegevens uit de grijze gebieden op een dusdanige wijze te groeperen dat zij volgens een voldoende scherp criterium kunnen worden geclassificeerd als wel of geen inhoud betreffend? De analyse in dit rapport heeft geen eenvoudig afbakeningscriterium opgeleverd aan de hand waarvan een logische typologie kan worden geformuleerd die eenduidig verkeersgegevens indeelt in gegevens die wel en gegevens die niet volgens het beschermingsregime van inhoud onder artikel 13 Gw beschermd moeten worden. Wel is het mogelijk om typen verkeersgegevens te ordenen aan de hand van bepaalde criteria, waarmee het afbakeningsprobleem wordt verkleind of in elk geval meer inzichtelijk wordt gemaakt. Zo kunnen verkeersgegevens worden ingedeeld naar de manier waarop zij mogelijk samenhangen met inhoud, volgens het semiotische onderscheid in soorten tekenrelaties. Verkeersgegevens die een afbeelding of diagram vormen van de inhoud of die indexicaal verwijzen naar inhoud, hebben over het algemeen een nauwer verband dan verkeersgegevens die metaforisch of symbolisch verwijzen naar inhoud. Dit biedt een zinvol materieel criterium, maar het is wel vrij abstract en vergt de nodige interpretatie. Een tweede mogelijkheid is een indeling naar het doel van de

verwerking, waarmee bestaande juridische categorieën verkeersgegevens kunnen worden geclassificeerd en waarbij bepaalde typen gegevens uitgesloten kunnen worden omdat zij niet met inhoud samenhangen. Een derde mogelijkheid is om verkeersgegevens in te delen naar privacygevoeligheid; omdat kennisneming van verkeersgegevens een verkillend effect kan hebben op de vrijheid om privé te communiceren, kunnen de meer privacygevoelige categorieën verkeersgegevens onder artikel 13 Gw worden beschermd, mogelijk op hetzelfde niveau als inhoud.

Geen van deze drie typologieën levert een ideale of eenduidige afbakening op, maar zij kunnen wel worden gecombineerd. Dat levert een stroomschema op van vijf vragen:

1. Valt het gegeven onder verantwoordelijkheid van de communicatiepartner(s)?
   Zo ja → inhoud. Zo nee → ga naar vraag 2.
2. Biedt het verkeersgegeven mogelijk zicht op de inhoud?
   Zo nee → verkeersgegeven. Zo ja → ga naar vraag 3.
3. Houdt het verkeersgegeven verband met een concrete communicatiehandeling?
   Zo nee → verkeersgegeven. Zo ja → ga naar vraag 4.
4. Is het een verkeersgegeven behorend bij telefonie (maar geen locatiegegeven)?
   Zo ja → verkeersgegeven. Zo nee → ga naar vraag 5.
5. Heeft het verkeersgegeven een sterke relatie met de inhoud? Er is een sterke relatie als het verkeersgegeven semiotisch een afbeelding, diagram, index, sterke metafoor of een sterk symbool is van de inhoud.
   Zo ja → inhoud. Zo nee → verkeersgegeven.

Aan de hand hiervan kunnen in beginsel alle categorieën verkeersgegevens worden ingedeeld naar inhoud of (pure) verkeersgegevens. In Tabel 5 in hoofdstuk 5 is een overzicht gegeven van wat deze classificatie oplevert voor concrete categorieën, waarbij een onderscheid gemaakt kan worden tussen telefonie, email en (overig) Internet. Bij Internetcommunicatie (buiten email) blijkt daarbij een complex beeld te bestaan wat verkeersgegevens wel of niet over communicatie-inhoud kunnen zeggen, zodat het moeilijk is om subcategorieën te definiëren die integraal als puur verkeersgegeven kunnen worden beschouw. Vaak zal de combinatie van verschillende gegevens het nodige suggereren over wat er is gecommuniceerd. Bovendien is het, aldus de technische analyse van Jan Smits, door de dynamiek en diversiteit van Internetprotocollen nauwelijks werkbaar om verkeersgegevens zinvol te scheiden van inhoud. Om die reden zouden verkeersgegevens bij Internetcommunicatie (met uitzondering van email) integraal als inhoud moeten worden behandeld.

Op een iets hoger abstractieniveau (dat wenselijk is voor de grondwetgever), kan de afbakening die volgt uit het stroomschema als volgt in meer algemene zin worden samengevat. In beginsel is een tweeledig afbakeningscriterium te formuleren dat juridisch voldoende abstractieniveau heeft en dat inhoudelijk goed werkt om de kern van het onderscheid tussen inhoud en verkeersgegevens te duiden. Het **hoofdcriterium** is onder wiens verantwoordelijkheid de gegevens vallen: inhoud is datgene wat onder verantwoordelijkheid van de verzender valt; verkeersgegevens zijn gegevens die onder verantwoordelijkheid van de transporteur (als transporteur) vallen. Het **nevencriterium** is dat verkeersgegevens die (juridisch-)technisch onder het begrip verkeersgegevens vallen, onder artikel 13 Gw als inhoud moeten worden behandeld wanneer zij de strekking weergeven van (een deel van) datgene wat valt onder de verantwoordelijkheid van de verzender. Het nevencriterium kan daarbij als volgt worden toegepast:[158]

- verkeersgegevens behorend bij telefonie die onder het beschermingsregime van verkeersgegevens vallen, kunnen limitatief worden opgesomd (bijvoorbeeld: nummer verzender/ontvanger, datum/tijdstip/duur, soort dienst); de overige telefoniegerelateerde verkeersgegevens vallen onder het beschermingsregime van inhoud;
    - locatiegegevens bij mobiele telefonie vormen een sui generis-categorie die te contextafhankelijk is om in te delen naar inhoud/verkeersgegeven; hiervoor dient de wetgever een zelfstandige keuze te maken;
- verkeersgegevens behorend bij email die onder het beschermingsregime van verkeersgegevens vallen, kunnen limitatief worden opgesomd (bijvoorbeeld: emailadres

[158] Hierbij laat ik verkeersgegevens behorend bij post buiten beschouwing, omdat deze geen reguleringsprobleem opleveren. De huidige wetgeving in de Postwet en het Wetboek van Strafvordering zouden gewoon kunnen worden gehandhaafd.

verzender/ontvanger, datum/tijdstip, volume); de overige emailgerelateerde verkeersgegevens vallen onder het beschermingsregime van inhoud;
- verkeersgegevens behorend bij Internet (met uitzondering van email) vallen integraal onder het beschermingsregime van inhoud.

Voor dit moment lijkt dit een indeling te bieden die recht doet aan de ratio van het correspondentiegeheim, voldoende abstractieniveau heeft vanuit het perspectief van de (grond)wetgever, en in de technisch-juridische werkelijkheid uitvoerbaar zou moeten zijn.

Bij deze conclusie passen echter twee kanttekeningen. De categorieën 'telefonie' en 'email' raken achterhaald nu alle communicatie in complexe patronen en met een grote diversiteit aan applicaties en protocollen over Internet wordt getransporteerd. Vrijwel alle communicatie is tegenwoordig Internetcommunicatie. Naast de technische convergentie van infrastructuren en diversificatie van protocollen, vindt er ook een sociale convergentie plaats van 'gesprekken' en 'berichtenverkeer', en tegelijkertijd een diversificatie aan communicatievormen van mens tot mens, mens tot machine, en machine tot machine. Vroeg of laat zullen in dit communicatielandschap 'telefonie' en 'email' geen bijzonder betekenisvolle categorieën meer zijn, waardoor het hiervoor gesuggereerde aanwijzen van verkeersgegevens behorend bij telefonie en email een zinloze of eindeloos complexe exercitie wordt in historisch-analogisch redeneren. In het Internettijdperk verliest het conceptuele onderscheid tussen verkeersgegevens en inhoud sterk aan relevantie als het gaat om het secundaire gebruik (naast het pure transport) van de gegevens. De conclusie zou dan moeten luiden dat, wanneer alle communicatie over Internet gaat, verkeersgegevens en inhoud altijd samenvallen vanuit de ratio van het correspondentiegeheim, en dat het historisch gegroeide begrip 'verkeersgegevens' zijn langste tijd gehad heeft om het gebruik van communicatiegerelateerde gegevens te reguleren.[159]

In plaats van een onderscheid tussen verkeersgegevens en inhoud van communicatie, zou dan een onderscheid tussen gebruikersgegevens en communicatiegerelateerde gegevens gehanteerd kunnen worden om de reikwijdte van het correspondentiegeheim te omschrijven. Communicatiegerelateerde gegevens zijn gegevens die samenhangen met concrete communicatiehandelingen en raken daarom direct de vrijheid om vertrouwelijk te kunnen communiceren; deze vallen integraal onder artikel 13 Gw. Gebruikersgegevens zijn gegevens over het telecommunicatiegebruik in meer algemene zin: het betreft gegevens over de gebruiker, zoals welke telefoonnummers, emailadressen en IP-adressen iemand in gebruik heeft en factuurgegevens; ook geaggregeerde verkeersgegevens zouden onder het begrip 'gebruikersgegevens' kunnen worden geschaard. Deze gegevens raken de vrijheid vertrouwelijk te communiceren niet of nauwelijks, omdat ze niet samenhangen met concrete keuzes om gebruik te maken van een communicatiemiddel, en vallen daarom buiten de reikwijdte van artikel 13 Gw. Een onderscheid tussen communicatiegerelateerde gegevens en gebruikersgegevens zou voor de langere termijn een bruikbaarder afbakeningscriterium kunnen bieden dan een onderscheid tussen (niet inhoudgerelateerde) verkeersgegevens en inhoud van communicatie.

Tot slot moet echter ook een tweede kanttekening worden geplaatst, namelijk dat Internetcommunicatie niet langer een fenomeen is dat zich uitsluitend in de relationele privacy van het correspondentiegeheim laat vangen. Het Internet is verknoopt met alle aspecten van wat burgers zijn en doen, en dat zal met de ontwikkeling van het Internet der dingen alleen maar toenemen. Internetcommunicatie biedt een steeds indringender inzicht in de persoonlijke levenssfeer, ook zonder dat kennis wordt genomen van inhoud; daarnaast zijn inmiddels ook opgeslagen gegevens (die losstaan van communicatie in de zin van relationele privacy) kwetsbaar voor kennisneming door derden. Informatie- en communicatietechnologie roept aldus vragen op over grondwettelijke bescherming van niet alleen de relationele privacy, maar ook de ruimtelijke en lichamelijke privacy. Het is daarom de vraag of er nog voldoende reden is om inhoud van communicatie als een zelfstandige categorie met meer egards te behandelen dan andere vormen van privacygevoelige gegevens in het digitale tijdperk. Voor de kortere termijn heeft het wellicht nog zin om communicatie-inhoud – met inbegrip van verkeersgegevens die

[159] Voor verkeersgegevens bij post zou een uitzondering kunnen worden gemaakt, omdat de infrastructuren van post (fysieke pakketjes die in de fysieke brievenbus worden afgeleverd) en telecommunicatie (digitale pakketjes die via elektronische signalen worden afgeleverd) – voor zover het gaat om de infrastructuur van transport – niet convergeren.

nauw verband houden met die inhoud – bijzondere bescherming te verlenen ten opzichte van andere vormen van digitale kwetsbaarheid. Voor de langere termijn – en dat is een termijn die past bij het perspectief van de grondwetgever – is het ook noodzakelijk om de systematiek van de privacygrondrechten over de hele linie opnieuw te doordenken, om effectief tegenwicht te bieden aan alle nieuwe vormen waarin de overheid zicht kan krijgen op de persoonlijke levenssfeer van burgers.

Over de auteur

Prof.dr. Bert-Jaap Koops is hoogleraar regulering van technologie bij TILT, het Tilburg Institute for Law, Technology, and Society van de Universiteit van Tilburg. Van 2005-2010 was hij lid van De Jonge Akademie, een onderdeel van de Koninklijke Nederlandse Akademie van Wetenschappen.

Koops doet onderzoek naar regulering en technologie, in het bijzonder strafrechtelijke onderwerpen als opsporingsbevoegdheden en privacy, computercriminaliteit, cryptografie en DNA. Hij is ook geïnteresseerd in andere onderwerpen binnen technologieregulering, zoals identificatie, dataprotectie, digitale grondrechten, regulering door techniek, de maakbare mens, en regulering van bio-, nano- en neurotechnologie. Van 2004-2009 leidde hij een VIDI-onderzoeksprogramma over recht, technologie en schuivende machtsverhoudingen.

Koops studeerde wiskunde en algemene literatuurwetenschap in Groningen. Hij promoveerde in 1999 in de rechtswetenschappen op een onderzoek naar regulering van cryptografie. Koops is co-redacteur van zeven boeken over technologieregulering, *Emerging Electronic Highways* (1996), *ICT Law and Internationalisation* (2000), *Starting Points for ICT Regulation* (2006), *Cybercrime and Jurisdiction* (2006), *Constitutional Rights and New Technologies* (2008), *Dimensions of Technology Regulation* (2010) en *Engineering the Human* (2013). Hij publiceerde diverse boeken en vele artikelen over recht en technologie. Zijn webpublicatie *Crypto Law Survey* wordt wereldwijd beschouwd als een standaardbron over cryptografie-regulering.

Literatuurlijst

Agre, P.E. (1998), 'Introduction', in: P.E. Agre en M. Rotenberg. *Technology and Privacy: The New Landscape*. Cambridge, MA / London: The MIT Press, p. 1-28.

Article 29 Working Party (2000), *Privacy on the Internet*, Brussels, Article 29 Data Protection Working Party, 21 November 2000.

Asscher, L. (2000), 'Trojaans hobbelpaard. Een analyse van het rapport van de commissie Grondrechten in het Digitale Tijdperk', *Mediaforum*(7/8), p. 228-233.

Asscher, L. (2003), *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam, Otto Cramwinckel.

Asscher, L.F. en A.H. Ekker (red.) (2003), *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam, Otto Cramwinckel Uitgever.

Blok, P. (2002), *Het recht op privacy*, Den Haag, Boom Juridische uitgevers.

Commissie Grondrechten in het digitale tijdperk (2000), *Rapport*, Den Haag, mei 2000,

Dommering, E.J. (1997), 'Geen telefoongeheim op de elektronische snelweg', *Mediaforum*(10), p. 142-147.

Dommering, E.J. (red.) (2000), *Informatierecht: fundamentele rechten voor de informatiesamenleving*, Amsterdam, O. Cramwinckel.

Ekker, A.H. (2003), 'Publiekrechtelijke bescherming van verkeersgegevens', in: L.F. Asscher en A.H. Ekker. *Verkeersgegevens. Een juridische en technische inventarisatie*. Amsterdam: Otto Cramwinckel Uitgever, p. 41-58.

Fischer, J.C. (2010), *Communications Network Traffic Data. Technical and Legal Aspects*, Eindhoven, TU/e.

Hes, R. (2003), 'Verkeersgegevens in nieuwe generaties telecommunicatiesystemen', in: L.F. Asscher en A.H. Ekker. *Verkeersgegevens. Een juridische en technische inventarisatie*. Amsterdam: Otto Cramwinckel Uitgever, p. 12-40.

Hildebrandt, M. (2008), 'Profiling and the Identity of the European citizen', in: M. Hildebrandt en S. Gutwirth. *Profiling the European Citizen*. s.l.: Springer, p. 303-326.

Hildebrandt, M. en S. Gutwirth (red.) (2008), *Profiling the European Citizen. Cross-disciplinary perspectives*, s.l., Springer.

Hofman, J.A. (1995). *Vertrouwelijke communicatie: een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht*, diss. Amsterdam (VU), Zwolle, W.E.J. Tjeenk Willink.

Koops, B.-J., G. Bodea , G. Broenink, et al. (2012a), *Juridische scan openbrononderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools*, Tilburg/Delft, TILT/TNO, juli 2012, 95 p.

Koops, B.-J., R. Leenes, P. De Hert, et al. (2012b), *Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing* Tilburg / Den Haag, TILT / WODC,

Koops, B.J. (2002), *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy*, Deventer, Kluwer, 335 p.

Koops, B.J. (2003), 'Verkeersgegevens en strafrecht: een agenda voor discussie', in: L.F. Asscher en A.H. Ekker. *Verkeersgegevens. Een juridische en technische inventarisatie*. Amsterdam: Otto Cramwinckel Uitgever, p. 59-92.

Lindenberg, K. (2002), *Van ORT tot ORO. Een verzameling van de werken die hebben geleid tot het Oorspronkelijk Regeringsontwerp van een nieuw Wetboek van Strafvordering (1914)*, Groningen, Rijksuniversiteit Groningen.

MacGillavry, E.C. (2004). *Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven*, diss. Groningen, Nijmegen, Wolf Legal Publishers.

Odinot, G., D. De Jong, J.B.J. Van der Leij, et al. (2012), *Het gebruik van de telefoon- en internettap in de opsporing*, Meppel, Boom Lemma, 302 p.

Patijn, A. (2004), 'Verplichte opslag van verkeersgegevens?', *Computerrecht*(2), p. 134-138.

Smits, A.H.H. (2006). *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen, Wolf Legal Publishers.

Smits, J.M. (2013), *Technische kwalificatie van verkeersgegvens ten behoeve van herziening artikel 13 Nederlandse Grondwet*, Utrecht, januari 2013.

Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, 2010.
Steenbruggen, W. (2009), *Publieke dimensies van privé-communicatie. Een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk*, Amsterdam, Otto Cramwinckel, 367 p.
Studiecommissie VMC (1999), 'Preadvies inzake een nieuwe tekst voor de artikelen 7 en 13 van de Grondwet', *Mediaforum*(11/12), p. 1-8.
Van Dorst, A.J.A. (1982), 'Het postgeheim', in: A.K. Koekkoek, W. Konijnenbelt en F.C.L.M. Crijns. *Grondrechten. Commentaar op Hoofdstuk 1 van de herziene Grondwet*. Nijmegen: Ars Aequi, p. 279-297.